Reverse Tunneling for Mobile IP, revised

Status of this Memo

Copyright Notice

Abstract

   Mobile Internet Protocol (IP) uses tunneling from the home agent to
   the mobile node's care-of address, but rarely in the reverse
   direction. Usually, a mobile node sends its packets through a router
   on the foreign network, and assumes that routing is independent of
   source address. When this assumption is not true, it is convenient
   to establish a topologically correct reverse tunnel from the care-of
   address to the home agent.

   This document proposes backwards-compatible extensions to Mobile IP
   to support topologically correct reverse tunnels. This document does
   not attempt to solve the problems posed by firewalls located between
   the home agent and the mobile node's care-of address.

   This document obsoletes RFC 2344.

Table of Contents

1. Introduction

   Section 1.3 of the Mobile IP specification [1] lists the following
   assumption:

      It is assumed that IP unicast datagrams are routed based on the
      destination address in the datagram header (i.e., not by source
      address).

   Because of security concerns (for example, IP spoofing attacks), and
   in accordance with RFC 2267 [8] and CERT [3] advisories to this
   effect, routers that break this assumption are increasingly more
   common.

   In the presence of such routers, the source and destination IP
   address in a packet must be topologically correct. The forward
   tunnel complies with this, as its endpoints (home agent address and
   care-of address) are properly assigned addresses for their respective
   locations. On the other hand, the source IP address of a packet
   transmitted by the mobile node does not correspond to the network
   prefix from where it emanates.

   This document discusses topologically correct reverse tunnels.

   Mobile IP does dictate the use of reverse tunnels in the context of
   multicast datagram routing and mobile routers. However, the source
   IP address is set to the mobile node's home address, so these tunnels
   are not topologically correct.

   Notice that there are several uses for reverse tunnels regardless of
   their topological correctness:

      - Mobile routers: reverse tunnels obviate the need for recursive
         tunneling [1].

      - Multicast: reverse tunnels enable a mobile node away from home
         to (1) join multicast groups in its home network, and (2)
         transmit multicast packets such that they emanate from its home
         network [1].

      - The TTL of packets sent by the mobile node (for example, when
         sending packets to other hosts in its home network) may be so
         low that they might expire before reaching their destination.
         A reverse tunnel solves the problem as it represents a TTL
         decrement of one [5].

1.1. Terminology

   The discussion below uses terms defined in the Mobile IP
   specification. Additionally, it uses the following terms:

      Forward Tunnel

         A tunnel that shuttles packets towards the mobile node. It
         starts at the home agent, and ends at the mobile node's care-of
         address.

      Reverse Tunnel

         A tunnel that starts at the mobile node's care-of address and
         terminates at the home agent.

   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 [9].

1.2. Assumptions

   Mobility is constrained to a common IP address space (that is, the
   routing fabric between, say, the mobile node and the home agent is
   not partitioned into a "private" and a "public" network).

   This document does not attempt to solve the firewall traversal
   problem. Rather, it assumes one of the following is true:

      - There are no intervening firewalls along the path of the
         tunneled packets.

      - Any intervening firewalls share the security association
         necessary to process any authentication [6] or encryption [7]
         headers which may have been added to the tunneled packets.

   The reverse tunnels considered here are symmetric, that is, they use
   the same configuration (encapsulation method, IP address endpoints)
   as the forward tunnel. IP in IP encapsulation [2] is assumed unless
   stated otherwise.

   Route optimization [4] introduces forward tunnels initiated at a
   correspondent host. Since a mobile node may not know if the
   correspondent host can decapsulate packets, reverse tunnels in that
   context are not discussed here.

1.3. Justification

   Why not let the mobile node itself initiate the tunnel to the home
   agent? This is indeed what it should do if it is already operating
   with a topologically correct co-located care-of address.

   However, one of the primary objectives of the Mobile IP specification
   is not to require this mode of operation.

   The mechanisms outlined in this document are primarily intended for
   use by mobile nodes that rely on the foreign agent for forward tunnel
   support. It is desirable to continue supporting these mobile nodes,
   even in the presence of filtering routers.

2. Overview

   A mobile node arrives at a foreign network, listens for agent
   advertisements and selects a foreign agent that supports reverse
   tunnels. It requests this service when it registers through the
   selected foreign agent. At this time, and depending on how the
   mobile node wishes to deliver packets to the foreign agent, it also
   requests either the Direct or the Encapsulating Delivery Style
   (section 5).

   In the Direct Delivery Style, the mobile node designates the foreign
   agent as its default router and proceeds to send packets directly to
   the foreign agent, that is, without encapsulation. The foreign agent
   intercepts them, and tunnels them to the home agent.

   In the Encapsulating Delivery Style, the mobile node encapsulates all
   its outgoing packets to the foreign agent. The foreign agent
   decapsulates and re-tunnels them to the home agent, using the foreign
   agent's care-of address as the entry-point of this new tunnel.

3. New Packet Formats

3.1. Mobility Agent Advertisement Extension

```
     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|   reserved     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                zero or more Care-of Addresses                 |
    |                           ...                                 |
```
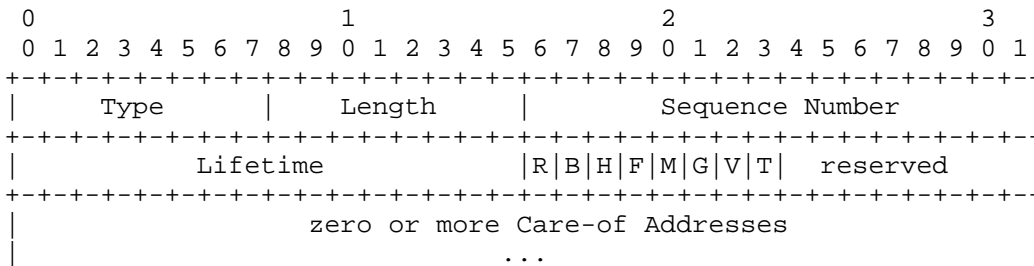
   The only change to the Mobility Agent Advertisement Extension [1] is
   the additional 'T' bit:

      T   Agent offers reverse tunneling service.

   A foreign agent that sets the 'T' bit MUST support the Direct
   Delivery Style. Encapsulating Delivery Style SHOULD be supported as
   well (section 5).

   Using this information, a mobile node is able to choose a foreign
   agent that supports reverse tunnels. Notice that if a mobile node
   does not understand this bit, it simply ignores it as per [1].

3.2. Registration Request

   Reverse tunneling support is added directly into the Registration
   Request by using one of the "rsvd" bits. If a foreign or home agent
   that does not support reverse tunnels receives a request with the 'T'
   bit set, the Registration Request fails. This results in a
   registration denial (failure codes are specified in section 3.4).

   Home agents SHOULD NOT object to providing reverse tunnel support,
   because they "SHOULD be able to decapsulate and further deliver
   packets addressed to themselves, sent by a mobile node" [1]. In the
   case of topologically correct reverse tunnels, the packets are not
   sent by the mobile node as distinguished by its home address.
   Rather, the outermost (encapsulating) IP source address on such
   datagrams is the care-of address of the mobile node.

   In Registration Requests sent by a mobile node, the Time to Live
   field in the IP header MUST be set to 255. This limits a denial of
   service attack in which malicious hosts send false Registration
   Requests (see Section 6).

```
      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|T|-|            Lifetime           |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                         Home Address                         |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                          Home Agent                          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                        Care-of Address                       |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                        Identification                        |
     |                                                              |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | Extensions ...
     +-+-+-+-+-+-+-+-
```
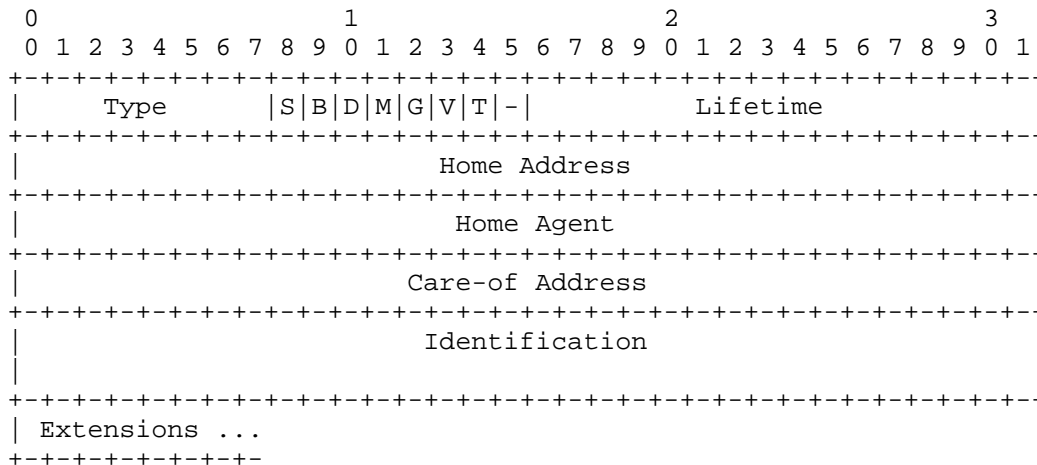
The only change to the Registration Request packet is the additional
'T' bit:

T   If the 'T' bit is set, the mobile node asks its home
          agent to accept a reverse tunnel from the care-of
          address. Mobile nodes using a foreign agent care-of
          address ask the foreign agent to reverse-tunnel its
          packets.

3.3. Encapsulating Delivery Style Extension

The Encapsulating Delivery Style Extension MAY be included by the
mobile node in registration requests to further specify reverse
tunneling behavior. It is expected to be used only by the foreign
agent. Accordingly, the foreign agent MUST consume this extension
(that is, it must not relay it to the home agent or include it in
replies to the mobile node). As per Section 3.6.1.3 of [1], the
mobile node MUST include the Encapsulating Delivery Style Extension
after the Mobile-Home Authentication Extension, and before the
Mobile-Foreign Authentication Extension, if present.

The Encapsulating Delivery Style Extension MUST NOT be included if
the 'T' bit is not set in the Registration Request.

If this extension is absent, Direct Delivery is assumed.
Encapsulation is done according to what was negotiated for the
forward tunnel (that is, IP in IP is assumed unless specified
otherwise). For more details on the delivery styles, please refer to
section 5.

   Foreign agents SHOULD support the Encapsulating Delivery Style
   Extension.

```
 0                       1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

     Type

         130

     Length

         0
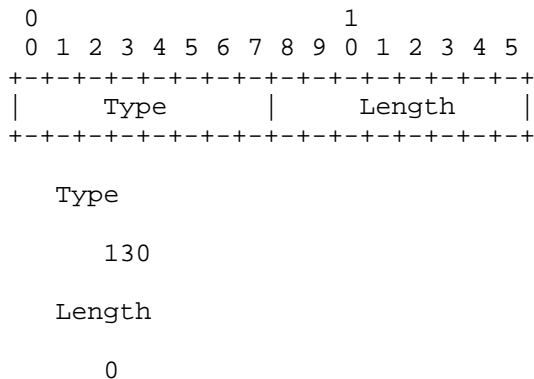
3.4. New Registration Reply Codes

   Foreign and home agent registration replies MUST convey if the
   reverse tunnel request failed. These new reply codes are defined:

      Service denied by the foreign agent:

      74 requested reverse tunnel unavailable
      75 reverse tunnel is mandatory and 'T' bit not set
      76 mobile node too distant
      79 delivery style not supported

      NOTE: Code 79 has not yet been assigned by IANA.

   and

      Service denied by the home agent:

      137 requested reverse tunnel unavailable
      138 reverse tunnel is mandatory and 'T' bit not set
      139 requested encapsulation unavailable

   In response to a Registration Request with the 'T' bit set, mobile
   nodes may receive (and MUST accept) code 70 (poorly formed request)
   from foreign agents and code 134 (poorly formed request) from home
   agents. However, foreign and home agents that support reverse
   tunneling MUST use codes 74 and 137, respectively.

   In addition to setting the 'T' bit, the mobile node also MAY request
   the Encapsulating Delivery Style by including the corresponding
   extension. If a foreign agent does not implement the Encapsulating

Delivery Style, it MUST respond to the mobile node with code 79
(delivery style not supported). This also applies if the foreign
agent does not support a requested delivery style that may be defined
in the future.

Absence of the 'T' bit in a Registration Request MAY elicit denials
with codes 75 and 138 at the foreign agent and the home agent,
respectively.

Forward and reverse tunnels are symmetric, that is, both are able to
use the same tunneling options negotiated at registration. This
implies that the home agent MUST deny registrations if an unsupported
form of tunneling is requested (code 139). Notice that Mobile IP [1]
already defines the analogous failure code 72 for use by the foreign
agent.

4. Changes in Protocol Behavior

Unless otherwise specified, behavior specified by Mobile IP [1] is
assumed. In particular, if any two entities share a mobility
security association, they MUST use the appropriate Authentication
Extension (Mobile-Foreign, Foreign-Home or Mobile-Home Authentication
Extension) when exchanging registration protocol datagrams. An
admissible authentication extension (for example the Mobile-Home
Authentication Extension) MUST always be present to authenticate
registration messages between a mobile node and its home agent.

Reverse tunneling imposes additional protocol processing requirements
on mobile entities. Differences in protocol behavior with respect to
Mobile IP [1] are specified in the subsequent sections.

4.1. Mobile Node Considerations

This section describes how the mobile node handles registrations that
request a reverse tunnel.

4.1.1. Sending Registration Requests to the Foreign Agent

In addition to the considerations in [1], a mobile node sets the 'T'
bit in its Registration Request to petition a reverse tunnel.

The mobile node MUST set the TTL field of the IP header to 255. This
is meant to limit the reverse tunnel hijacking attack (Section 6).

The mobile node MAY optionally include an Encapsulating Delivery
Style Extension.

4.1.2. Receiving Registration Replies from the Foreign Agent

   Possible valid responses are:

      - A registration denial issued by either the home agent or the
        foreign agent:

        a. The mobile node follows the error checking guidelines in
           [1], and depending on the reply code, MAY try modifying the
           registration request (for example, by eliminating the
           request for alternate forms of encapsulation or delivery
           style), and issuing a new registration.

        b. Depending on the reply code, the mobile node MAY try zeroing
           the 'T' bit, eliminating the Encapsulating Delivery Style
           Extension (if one was present), and issuing a new
           registration. Notice that after doing so the registration
           may succeed, but due to the lack of a reverse tunnel data
           transfer may not be possible.

      - The home agent returns a Registration Reply indicating that the
        service will be provided.

   In this last case, the mobile node has succeeded in establishing a
   reverse tunnel between its care-of address and its home agent. If
   the mobile node is operating with a co-located care-of address, it
   MAY encapsulate outgoing data such that the destination address of
   the outer header is the home agent. This ability to selectively
   reverse-tunnel packets is discussed further in section 5.4.

   If the care-of address belongs to a separate foreign agent, the
   mobile node MUST employ whatever delivery style was requested (Direct
   or Encapsulating) and proceed as specified in section 5.

   A successful registration reply is an assurance that both the foreign
   agent and the home agent support whatever alternate forms of
   encapsulation (other than IP in IP) were requested. Accordingly, the
   mobile node MAY use them at its discretion.

4.2. Foreign Agent Considerations

   This section describes how the foreign agent handles registrations
   that request a reverse tunnel.

4.2.1. Receiving Registration Requests from the Mobile Node

   A foreign agent that receives a Registration Request with the 'T' bit
   set processes the packet as specified in the Mobile IP specification
   [1], and determines whether it can accommodate the forward tunnel
   request. If it cannot, it returns an appropriate code. In
   particular, if the foreign agent is unable to support the requested
   form of encapsulation it MUST return code 72. If it cannot support
   the requested form of delivery style it MUST return code 79 (delivery
   style not supported).

   The foreign agent MAY reject Registration Requests without the 'T'
   bit set by denying them with code 75 (reverse tunnel is mandatory and
   'T' bit not set).

   The foreign agent MUST verify that the TTL field of the IP header is
   set to 255. Otherwise, it MUST reject the registration with code 76
   (mobile node too distant). The foreign agent MUST limit the rate at
   which it sends these registration replies to a maximum of one per
   second.

   As a last check, the foreign agent verifies that it can support a
   reverse tunnel with the same configuration. If it cannot, it MUST
   return a Registration Reply denying the request with code 74
   (requested reverse tunnel unavailable).

4.2.2. Relaying Registration Requests to the Home Agent

   Otherwise, the foreign agent MUST relay the Registration Request to
   the home agent.

   Upon receipt of a Registration Reply that satisfies validity checks,
   the foreign agent MUST update its visitor list, including indication
   that this mobile node has been granted a reverse tunnel and the
   delivery style expected (section 5).

   While this visitor list entry is in effect, the foreign agent MUST
   process incoming traffic according to the delivery style, encapsulate
   it and tunnel it from the care-of address to the home agent's
   address.

4.3. Home Agent Considerations

   This section describes how the home agent handles registrations that
   request a reverse tunnel.

4.3.1. Receiving Registration Requests from the Foreign Agent

   A home agent that receives a Registration Request with the 'T' bit
   set processes the packet as specified in the Mobile IP specification
   [1] and determines whether it can accommodate the forward tunnel
   request. If it cannot, it returns an appropriate code. In
   particular, if the home agent is unable to support the requested form
   of encapsulation it MUST return code 139 (requested encapsulation
   unavailable).

   The home agent MAY reject registration requests without the 'T' bit
   set by denying them with code 138 (reverse tunnel is mandatory and '
   T' bit not set).

   As a last check, the home agent determines whether it can support a
   reverse tunnel with the same configuration as the forward tunnel. If
   it cannot, it MUST send back a registration denial with code 137
   (requested reverse tunnel unavailable).

   Upon receipt of a Registration Reply that satisfies validity checks,
   the home agent MUST update its mobility bindings list to indicate
   that this mobile node has been granted a reverse tunnel and the type
   of encapsulation expected.

4.3.2. Sending Registration Replies to the Foreign Agent

   In response to a valid Registration Request, a home agent MUST issue
   a Registration Reply to the mobile node.

   After a successful registration, the home agent may receive
   encapsulated packets addressed to itself. Decapsulating such packets
   and blindly injecting them into the network is a potential security
   weakness (section 6.1). Accordingly, the home agent MUST implement,
   and, by default, SHOULD enable the following check for encapsulated
   packets addressed to itself:

      The home agent searches for a mobility binding whose care-of
      address is the source of the outer header, and whose mobile node
      address is the source of the inner header.

   If no such binding is found, or if the packet uses an encapsulation
   mechanism that was not negotiated at registration the home agent MUST
   silently discard the packet and SHOULD log the event as a security
   exception.

   Home agents that terminate tunnels unrelated to Mobile IP (for
   example, multicast tunnels) MAY turn off the above check, but this
   practice is discouraged for the aforementioned reasons.

While the registration is in effect, a home agent MUST process each
valid reverse tunneled packet (as determined by checks like the
above) by decapsulating it, recovering the original packet, and then
forwarding it on behalf of its sender (the mobile node) to the
destination address (the correspondent host).

5. Mobile Node to Foreign Agent Delivery Styles

   This section specifies how the mobile node sends its data traffic via
   the foreign agent. In all cases, the mobile node learns the foreign
   agent's link-layer address from the link-layer header in the agent
   advertisement.

5.1. Direct Delivery Style

   This delivery mechanism is very simple to implement at the mobile
   node, and uses small (non-encapsulated) packets on the link between
   the mobile node and the foreign agent (potentially a very slow link).
   However, it only supports reverse-tunneling of unicast packets, and
   does not allow selective reverse tunneling (section 5.4).

5.1.1. Packet Processing

   The mobile node MUST designate the foreign agent as its default
   router. Not doing so will not guarantee encapsulation of all the
   mobile node's outgoing traffic, and defeats the purpose of the
   reverse tunnel. The foreign agent MUST:

     - detect packets sent by the mobile node, and

     - modify its forwarding function to encapsulate them before
        forwarding.

5.1.2. Packet Header Format and Fields

   This section shows the format of the packet headers used by the
   Direct Delivery style. The formats shown assume IP in IP
   encapsulation [2].

   Packet format received by the foreign agent (Direct Delivery Style):

      IP fields:
        Source Address = mobile node's home address
        Destination Address = correspondent host's address
      Upper Layer Protocol

   Packet format forwarded by the foreign agent (Direct Delivery Style):

```
      IP fields (encapsulating header):
        Source Address = foreign agent's care-of address
        Destination Address = home agent's address
        Protocol field: 4 (IP in IP)
      IP fields (original header):
        Source Address = mobile node's home address
        Destination Address = correspondent host's address
      Upper Layer Protocol
```

   These fields of the encapsulating header MUST be chosen as follows:

      IP Source Address

         Copied from the Care-of Address field within the Registration
         Request.

      IP Destination Address

         Copied from the Home Agent field within the most recent
         successful Registration Reply.

      IP Protocol Field

         Default is 4 (IP in IP [2]), but other methods of encapsulation
         MAY be used as negotiated at registration time.

5.2. Encapsulating Delivery Style

   This mechanism requires that the mobile node implement encapsulation,
   and explicitly directs packets at the foreign agent by designating it
   as the destination address in a new outermost header. Mobile nodes
   that wish to send either broadcast or multicast packets MUST use the
   Encapsulating Delivery Style.

5.2.1 Packet Processing

   The foreign agent does not modify its forwarding function. Rather,
   it receives an encapsulated packet and after verifying that it was
   sent by the mobile node, it:

      - decapsulates to recover the inner packet,

      - re-encapsulates, and sends it to the home agent.

   If a foreign agent receives an un-encapsulated packet from a mobile
   node which had explicitly requested the Encapsulated Delivery Style,
   then the foreign agent MUST NOT reverse tunnel such a packet and
   rather MUST forward it using standard, IP routing mechanisms.

5.2.2. Packet Header Format and Fields

   This section shows the format of the packet headers used by the
   Encapsulating Delivery style. The formats shown assume IP in IP
   encapsulation [2].

   Packet format received by the foreign agent (Encapsulating Delivery
   Style):

      IP fields (encapsulating header):
        Source Address = mobile node's home address
        Destination Address = foreign agent's address
        Protocol field: 4 (IP in IP)
      IP fields (original header):
        Source Address = mobile node's home address
        Destination Address = correspondent host's address
      Upper Layer Protocol

   The fields of the encapsulating IP header MUST be chosen as follows:

      IP Source Address

        The mobile node's home address.

      IP Destination Address

        The address of the agent as learned from the IP source address
        of the agent's most recent successful registration reply.

      IP Protocol Field

        Default is 4 (IP in IP [2]), but other methods of encapsulation
        MAY be used as negotiated at registration time.

   Packet format forwarded by the foreign agent (Encapsulating Delivery
   Style):

      IP fields (encapsulating header):
        Source Address = foreign agent's care-of address
        Destination Address = home agent's address
        Protocol field: 4 (IP in IP)
      IP fields (original header):
        Source Address = mobile node's home address
        Destination Address = correspondent host's address
      Upper Layer Protocol

   These fields of the encapsulating IP header MUST be chosen as
   follows:

     IP Source Address

        Copied from the Care-of Address field within the Registration
        Request.

     IP Destination Address

        Copied from the Home Agent field within the most recent
        successful Registration Reply.

     IP Protocol Field

        Default is 4 (IP in IP [2]), but other methods of encapsulation
        MAY be used as negotiated at registration time.

5.3. Support for Broadcast and Multicast Datagrams

   If a mobile node is operating with a co-located care-of address,
   broadcast and multicast datagrams are handled according to Sections
   4.3 and 4.4 of the Mobile IP specification [1]. Mobile nodes using a
   foreign agent care-of address MAY have their broadcast and multicast
   datagrams reverse-tunneled by the foreign agent. However, any mobile
   nodes doing so MUST use the encapsulating delivery style.

   This delivers the datagram only to the foreign agent. The latter
   decapsulates it and then processes it as any other packet from the
   mobile node, namely, by reverse tunneling it to the home agent.

5.4. Selective Reverse Tunneling

   Packets destined to local resources (for example, a nearby printer)
   might be unaffected by ingress filtering. A mobile node with a co-
   located care-of address MAY optimize delivery of these packets by not
   reverse tunneling them. On the other hand, a mobile node using a
   foreign agent care-of address MAY use this selective reverse
   tunneling capability by requesting the Encapsulating Delivery Style,
   and following these guidelines:

     Packets NOT meant to be reversed tunneled:

        Sent using the Direct Delivery style. The foreign agent MUST
        process these packets as regular traffic: they MAY be
        forwarded but MUST NOT be reverse tunneled to the home agent.

      Packets meant to be reverse tunneled:

          Sent using the Encapsulating Delivery style. The foreign agent
          MUST process these packets as specified in section 5.2: they
          MUST be reverse tunneled to the home agent.

6. Security Considerations

   The extensions outlined in this document are subject to the security
   considerations outlined in the Mobile IP specification [1].
   Essentially, creation of both forward and reverse tunnels involves an
   authentication procedure, which reduces the risk for attack.

6.1. Reverse-tunnel Hijacking and Denial-of-Service Attacks

   Once the tunnel is set up, a malicious node could hijack it to inject
   packets into the network. Reverse tunnels might exacerbate this
   problem, because upon reaching the tunnel exit point packets are
   forwarded beyond the local network. This concern is also present in
   the Mobile IP specification, as it already dictates the use of
   reverse tunnels for certain applications.

   Unauthenticated exchanges involving the foreign agent allow a
   malicious node to pose as a valid mobile node and re-direct an
   existing reverse tunnel to another home agent, perhaps another
   malicious node. The best way to protect against these attacks is by
   employing the Mobile-Foreign and Foreign-Home Authentication
   Extensions defined in [1].

   If the necessary mobility security associations are not available,
   this document introduces a mechanism to reduce the range and
   effectiveness of the attacks. The mobile node MUST set to 255 the
   TTL value in the IP headers of Registration Requests sent to the
   foreign agent. This prevents malicious nodes more than one hop away
   from posing as valid mobile nodes. Additional codes for use in
   registration denials make those attacks that do occur easier to
   track.

   With the goal of further reducing the attacks the Mobile IP Working
   Group considered other mechanisms involving the use of
   unauthenticated state. However, these introduce the possibilities of
   denial-of-service attacks. The consensus was that this was too much
   of a trade-off for mechanisms that guarantee no more than weak (non-
   cryptographic) protection against attacks.

6.2. Ingress Filtering

   There has been some concern regarding the long-term effectiveness of
   reverse-tunneling in the presence of ingress filtering. The
   conjecture is that network administrators will target reverse-
   tunneled packets (IP in IP encapsulated packets) for filtering. The
   ingress filtering recommendation spells out why this is not the case
   [8]:

      Tracking the source of an attack is simplified when the source is
      more likely to be "valid."

6.3. Reverse Tunneling for Disparate Address Spaces

   There are security implications involved with the foreign agent's
   using link-layer information to select the proper reverse tunnel for
   mobile node packets (section A.3). Unauthenticated link-layers allow
   a malicious mobile node to misuse another's existing reverse tunnel,
   and inject packets into the network.

   For this solution to be viable, the link-layer MUST securely
   authenticate traffic received by the foreign agent from the mobile
   nodes. Unauthenticated link-layer technologies (for example shared
   ethernet) are not recommended to implement disparate address support.

7. IANA Considerations

   The Encapsulating Delivery Style extension defined in section 3.3 is
   a Mobile IP registration extension as defined in [1]. IANA assigned
   the value of 130 for this purpose at the time of the publication of
   RFC 2344.

   The Code values defined in section 3.4 are error codes as defined in
   [1]. They correspond to error values associated with rejection by
   the home and foreign agents. At the time of the publication of RFC
   2344, IANA assigned codes 74-76 for the foreign agent rejections and
   codes 137-139 for the home agent rejections. The code for 'delivery
   style not supported' has been assigned a value of 79 by the IANA for
   this purpose.

8. Acknowledgements

   The encapsulating style of delivery was proposed by Charlie Perkins.
   Jim Solomon has been instrumental in shaping this document into its
   present form. Thanks to Samita Chakrabarti for helpful comments on
   disparate address space support, and for most of the text in section
   A.4.

References

   [1] Perkins, C., "IP Mobility Support", RFC 2002, October 1996.

   [2] Perkins, C., "IP Encapsulation within IP", RFC 2003, October
        1996.

   [3] Computer Emergency Response Team (CERT), "IP Spoofing Attacks
        and Hijacked Terminal Connections", CA-95:01, January 1995.
        Available via anonymous ftp from info.cert.org in
        /pub/cert_advisories.

   [4] Perkins, C. and D. Johnson, "Route Optimization in Mobile IP",
        Work in Progress.

   [5] Manuel Rodriguez, private communication, August 1995.

   [6] Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402,
        November 1998.

   [7] Kent, S. and R. Atkinson, "IP Encapsulating Payload", RFC 2406,
        November 1998.

   [8] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating
        Denial of Service Attacks which employ IP Source Address
        Spoofing", RFC 2267, January 1998.

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

   [10] Farinacci, D., Li, T., Hanks, S., Meyer, D. and P. Traina,
        "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

   [11] Aboba, B. and M. Beadles, "The Network Access Identifier", RFC
        2486, January 1999.

   [12] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G.J. and
        E. Lear, "Address Allocation for Private Internets", BCP 5, RFC
        1918, February 1996.

   [13] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC
        2890, August 2000.

Editor and Chair Addresses

   Questions about this document may be directed at:

   Gabriel E. Montenegro
   Sun Microsystems
   Laboratories, Europe
   29, chemin du Vieux Chene
   38240 Meylan
   FRANCE

   Phone: +33 476 18 80 45
   EMail: gab@sun.com

   The working group can be contacted via the current chairs:

   Basavaraj Patil
   Nokia Networks
   6000 Connection Drive
   Irving, TX 75039
   USA

   Phone: +1 972-894-6709
   Fax :   +1 972-894-5349
   EMail: Raj.Patil@nokia.com

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

   Phone: +1 847-632-3148
   EMail: QA3445@email.mot.com

Appendix A: Disparate Address Space Support

   Mobile IP [1] assumes that all the entities involved (mobile
   node, foreign agent and home agent) have addresses within the
   same globally routable address space. In many deployment
   scenarios, when a mobile node leaves its home network it may
   wander into a region where its home address is not routable or
   known by the local routing fabric. Similarly, the IP addresses
   of the foreign agent and the home agent may belong to disparate
   address spaces, which precludes their exchanging registration
   protocol messages directly. These issues are possible
   particularly if the entities involved use addresses from the
   ranges specified in RFC1918 [12] to support private networks.

   Accurately speaking, the use of private addresses is not the
   only cause. It may, in fact, be the most common, but the root of
   the problem lies in the use of disparate address spaces. For
   example, corporations often have several properly allocated
   address ranges. They typically advertise reachability to only a
   subset of those ranges, leaving the others for use exclusively
   within the corporate network. Since these ranges are not
   routable in the general Internet, their use leads to the same
   problems encountered with "private" addresses, even though they
   are not taken from the ranges specified in RFC1918.

   Even if the mobile node, home agent and foreign agent all reside
   within the same address space, problems may arise if the
   correspondent node does not. However, this problem is not
   specific to Mobile IP, and is beyond the scope of this
   document. The next section limits even further the scope of the
   issues relevant to this document. A subsequent section explains
   how reverse tunneling may be used to tackle them.

A.1. Scope of the Reverse Tunneling Solution

   Reverse tunneling (as defined in this document) may be used to
   cope with disparate address spaces, within the following
   constraints:

      - There are no provisions to solve the case in which the
         correspondent node and the mobile node are in disparate
         address spaces. This limits the scope of the problem to
         only those issues specific to Mobile IP.

      - The foreign agent and the home agent are directly reachable
         to each other by virtue of residing in the same address
         space. This limits the scope of the problem to only the
         simplest of cases. This also implies that the registration

protocol itself has a direct path between the foreign
agent and the home agent, and, in this respect, is not
affected by disparate address spaces. This restriction
also applies to mobile nodes operating with a co-located
care-of address. In this case, reverse tunneling is a
complete and elegant solution.

- There are no additional protocol elements beyond those
  defined by Mobile IP [1] and reverse tunneling. In
  particular, additional extensions to the registration
  requests or replies, or additional bits in the
  header--although potentially useful--are outside the scope
  of this document.

In spite of the limitations, reverse tunneling may be used to
solve the most common issues. The range of problems that can be
solved are best understood by looking at some simple diagrams:

Figure A1: NON-ROUTABLE PACKETS IN DISPARATE ADDRESS SPACES

```
   Mc                  Fa  Fb             Hb  Hc            Yc
[MN]-----------------[FA]----------------[HA]---------------[Y]
     Addr space A           Addr space B          Addr space C
```
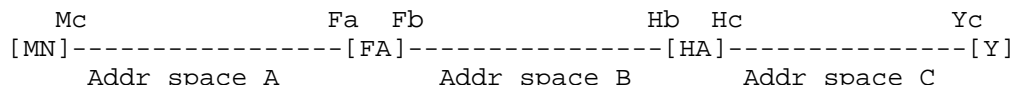
In this diagram, there are three disparate address spaces: A, B and
C. The home agent (HA) has one address each on address spaces B and
C, and the foreign agent (FA), on address spaces A and B. The mobile
node's (MN) has a permanent address, Mc, within address space C.

In the most common scenario both A and C are "private" address
spaces, and B is the public Internet.

Suppose MN sends a packet to correspondent node (Y) in its home
network. Presumably, MN has no difficulties delivering this packet
to the FA, because it does so using layer 2 mechanisms. Somehow, the
FA must realize that this packet must be reverse tunneled, and it
must fetch the proper binding to do so. Possible mechanisms are
outlined in section A.3.

However, once the packet is in address space B it becomes non-
routable. Note that ingress filtering only exacerbates the problem,
because it adds a requirement of topological significance to the
source IP address in addition to the that of the destination address.
As Mobile IP matures, others entities may be defined (for example,
AAA servers). Their addition places even more requirements on the
address spaces in use.

Reverse tunneling adds a topologically significant IP header to the
packet (source IP address of Fb, destination of Hb) during its
transit within address space B. Assuming IP in IP encapsulation
(although others, like GRE are also possible), this is what the
packet looks like:

     Figure A2: IP IN IP REVERSE TUNNELED PACKET FROM FA TO HA

```
            +-----------------+
            |         +-------+|
            | Fb->Hb  | Mc->Yc||
            |         +-------+|
            +--------+--------+
```

HA receives this packet, recovers the original packet, and since it
is cognizant of address space C, delivers it to the appropriate
interface.

Of course, for this to happen, the care-of address registered by the
MN is not the usual Fa, but Fb. How this happens is outside the
scope of this document. Some possible mechanisms are:

   - FA recognizes mobile nodes whose addresses fall within the
      private address ranges specified by RFC1918. In this case, the
      foreign agent could force the use of Fb as the care-of address,
      perhaps by rejecting the initial registration request with an
      appropriate error message and supplemental information.

   - FA could be configured to always advertise Fb as long as H->Fb
      and Fb->H are guaranteed to be valid forward and reverse
      tunnels, respectively, for all values of H. Here, H is the
      address of any home agent whose mobile nodes may register via
      FA.

   - FA could indicate that it supports disparate address spaces via
      a currently undefined 'P' bit in its advertisements, and an
      indication of the relevant address space for any or all of its
      care-of addressed by including an NAI [11] or a realm indicator
      (perhaps a variant of the NAI). Alternatively, mobile nodes so
      configured could solicit the NAI or realm indicator information
   in response to advertisements with the 'P' bit set.

Additionally, the mobile node needs to supply the appropriate address
for its home agent: Hb instead of the usual Hc. How this happens is
outside the scope of this document. Some possible mechanisms are:

   - This determination could be triggered in response to using the
      foreign agent's Fb as the care-of address.

        - The mobile node could always use Hb as its home agent address,
           specially (1) if Hb is routable within address space C, or (2)
           if MN is certain never to be at home (in some configurations,
           the mobile nodes are always roaming).

        - The mobile node could be configured with different home agent
           addresses and their corresponding address space (perhaps
           indicated via an NAI [11] or a variant of it).

   Another major issue introduced by private addresses is that of two or
   more mobile nodes with the same numeric IP address:

       Figure A3: MOBILE NODES WITH CONFLICTING ADDRESSES

```
              Mc=M                  H1b      H1c
         [MN1]-------+        +----[HA1]----+---------
                     |        |             | Address
                     |        |             | space C
         Address     |        |  Address    +---------
         Space     Fa-[FA]-Fb  Space
         A           |        |  B          +---------
                     |        |             | Address
                     |        |             | space D
         [MN2]-------+        +----[HA2]----+---------
              Md=M                  H2b      H2d
```
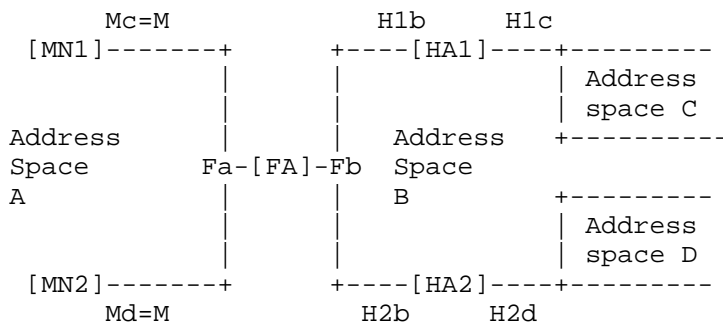
   Suppose there are two address spaces A and B, and a foreign agent
   (FA) with interfaces on both. There are two home agents (HA1 and
   HA2) in address space B, with addresses H1b and H2b, respectively.
   Each of the home agents has an interface in a private address space
   in addition to address space B: HA1 has H1c on C, and HA2 has H2d on
   D. MN1 and MN2 are two mobile nodes with home addresses Mc and Md,
   corresponding to address space C and D, respectively.

   If Mc and Md are private addresses as defined in RFC1918, they may be
   numerically equivalent (both equal to M). Because of this, the
   foreign agent can no longer rely on only the mobile node's home
   address to disambiguate amongst its different bindings.

A.2. Terminating Forward Tunnels at the Foreign Agent

   In figure A1, suppose the correspondent node Y sends a packet to the
   mobile node at address Mc. The packet is intercepted by the home
   agent at Hc and tunneled towards the mobile node via address Fb.

Once the packet reaches FA (via address Fb), the foreign agent must identify which of its registered mobile nodes is the ultimate destination for the internal packet. In order to do so, it needs to identify the proper binding via a tuple guaranteed to be unique among all of its mobile nodes.

The unique tuple sufficient for demultiplexing IP in IP packets [IPIP] (protocol 4) is:

   - destination IP address of the encapsulated (internal) header

     This is mobile node MN's home address (Mc in the above example). At first glance, it seems like this is unique among all mobile nodes, but as mentioned above, with private addresses another mobile may have an address Md numerically equivalent to Mc.

   - source IP address of the external header

     This, the remote end of the tunnel, is Hb in the above example.

   - destination IP address of the external header

     This, the local end of the tunnel, is Fb in the above example.

The three values above are learned from a successful registration and are the mobile node's home address, the home agent's address and the care-of address. Thus, it is possible to identify the right binding. Once FA identifies the ultimate destination of the packet, Mc, it delivers the internal packet using link layer mechanisms.

GRE packets [10] (protocol 47) are only handled if their Protocol Type field has a value of 0x800 (other values are outside the scope of this document), and are demultiplexed based on the same tuple as IP in IP packets. In GRE terminology, the tuple is:

   - destination IP address of the payload (internal) packet

   - source IP address of the delivery (external) packet

   - destination IP address of the delivery (external) packet

Notice that the Routing, Sequence Number, Strict Source Route and Key fields have been deprecated from GRE [10]. However, a separate document specifies their use [13].

The above tuples work for IP-in-IP or GRE encapsulation, and assume
that the inner packet is in the clear. Encapsulations which encrypt
the inner packet header are outside the scope of this document.

A.3. Initiating Reverse Tunnels at the Foreign Agent

In figure A3, suppose mobile node M1 sends a packet to a
correspondent node in its home address space, C, and mobile node M2
sends a packet to a correspondent node in its home address space, D.

At FA, the source addresses for both packets will be seen as M, thus
this is not sufficient information. The unique tuple required to
identify the proper binding is:

   - link-layer information related to the MN

      This may be in the form of a MAC address, a PPP session (or
      incoming interface) or channel coding for a digital cellular
      service. Device ID's can also be used in this context.

   - source IP address of the IP header.

      As was pointed out, this by itself is not guaranteed to be
   unique.

This information must be established and recorded at registration
time. The above items are sufficient for the foreign agent to select
the proper binding to use. This, in turn, produces the address of
the home agent, and the reverse tunneling options negotiated during
the registration process. The foreign agent can now proceed with
reverse tunneling.

A.4. Limited Private Address Scenario

The Limited Private Address Scenario (LPAS) has received much
attention from the cellular wireless industry, so it is useful to
define it and to clarify what its requirements are.

LPAS is a subset of the disparate address space scenario discussed in
this appendix. This section explains how LPAS could be deployed
given the current state of the Mobile IP specifications.

                    Figure A4: EXAMPLE PRIVATE ADDRESS SCENARIO

```
    10.10.1.2
    +----+                    IF1=COA1+-------+    HAA2 +-----+
    | MN1|------------------------|  FA   |---------| HA2 |
    +----+             +-----------|       |         +-----+
                       |    IF2=COA2+-------+    |
                +---+                         |
                |                             |
             +-----+                          |
             | MN2 |                          |
             +-----+                          |
              10.10.1.2                       |
                                              |
                                              |  HAA1
                                  +------+
                                  | HA1  |
                                  +------+
```
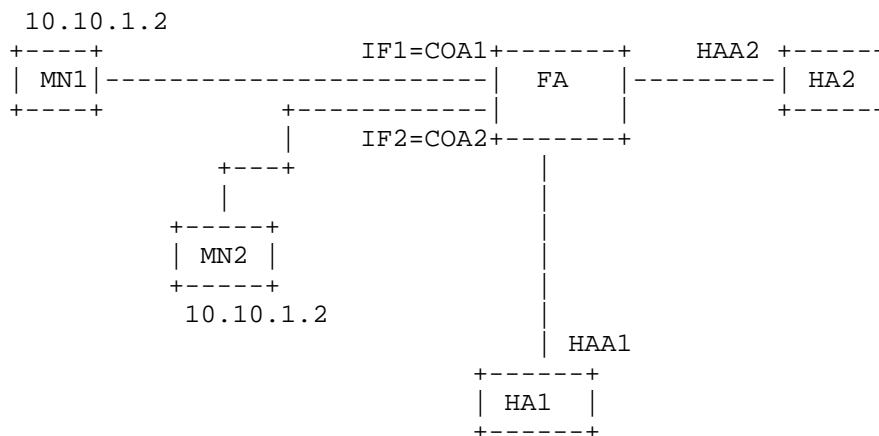
The above figure presents a very simple scenario in which private
addresses are used. Here, "private addresses" are strictly those
defined in RFC 1918 [12]. In this deployment scenario, the only
entities that have private addresses are the mobile nodes. Foreign
agent and home agent addresses are publicly routable on the general
Internet. More specifically, the care-of addresses advertised by the
foreign agents (COA1 and COA2 in Figure A4) and the home agent
addresses used by mobile nodes in registration requests (HAA1 and
HAA2 in Figure A4) are publicly routable on the general Internet. As
a consequence, any Mobile IP tunnels can be established between any
home agent home address and any foreign agent care-of address.

Also, note that two different mobile nodes (MN1 and MN2) with the
same private address (10.10.1.2) are visiting the same foreign agent
FA. This is supported as long as MN1 and MN2 are serviced by
different home agents. Hence, from any given home agent's
perspective, each mobile node has a unique IP address, even if it
happens to be a private address as per RFC 1918.

Operation in the presence of route optimization [4] is outside the
scope of this document.

Requirements for the above private address scenario:

   Mobile node requirements:

      Mobile nodes intending to use private addresses with Mobile IP
      MUST set the 'T' bit and employ reverse tunneling. Mobile
      node's private addresses within a given address space MUST be
      unique. Thus two mobile nodes belonging to a single home agent

cannot have the same private addresses. Thus, when receiving
or sending tunneled traffic for a mobile node, the tunnel
endpoints are used to disambiguate amongst conflicting mobile
node addresses.

If the mobile node happens to register with multiple home
agents simultaneously through the same foreign agent, there
must be some link-layer information that is distinct for each
mobile node. If no such distinct link-layer information is
available, the mobile nodes MUST use unique address.

Foreign agent requirements:

All advertising interfaces of the foreign agent MUST have
publicly routable care-of address. Thus, a mobile node with a
private address visits the foreign agent only in its publicly
routable network.

Foreign agents MUST support reverse tunneling in order to
support private addressed mobile nodes. If a foreign agent
receives a registration request from a mobile node with a
private address, and the mobile node has not set the 'T' bit,
the foreign agent SHOULD reject it.

When delivering packets to or receiving packets from mobile
nodes, foreign agents MUST disambiguate among mobile node with
conflicting private addresses by using link-layer information
as mentioned previously (Appendix section A.2 and A.3). A
foreign agent in absence of route optimization, should make
sure that two mobile nodes visiting the same foreign agent
corresponds with each other through their respective home
agents.

If a foreign agent supports reverse tunneling, then it MUST
support the simple scenario of private address support
described in this section.

Home agent requirements:

Any home agent address used by mobile nodes in registration
request MUST be a publicly routable address. Home agents will
not support overlapping private home addresses, thus each
private home address of a mobile node registered with a home
agent is unique. When the 'T' bit is set in the registration
request from the mobile node, the home agent MUST recognize and
accept registration request from mobile nodes with private

        addresses. Also, the home agent SHOULD be able to assign
        private addresses out of its address pool to mobile nodes for
        use as home addresses. This does not contravene home agent
        processing in section 3.8 of [1].

Appendix B: Changes from RFC2344

   This section lists the changes with respect to the previous version
   of this document (RFC2344).

   - Added Appendix A on support for Disparate Addresses spaces and
     private addresses.

   - Added the corresponding section (6.3) under 'Security
     Considerations'.

   - Made Encapsulating Delivery Support optional by demoting from
     a MUST to a should. This also required defining a new error
     code 79 (assigned by IANA).

   - Mentioned the possibility of an admissible authentication
     extension which may be different from the Mobile-Home
     authentication extension.

   - An IANA considerations section was added.

Full Copyright Statement

Acknowledgement