Internet Engineering Task Force
INTERNET DRAFT

G. Montenegro, Editor
Sun Microsystems, Inc.
January 26, 1998

Reverse Tunneling for Mobile IP
draft-ietf-mobileip-tunnel-reverse-05.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 Working Group mailing list at "mobile-ip@SmallWorks.COM".

Distribution of this memo is unlimited.

This document is an Internet-Draft. 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.''

To learn the current status of any Internet-Draft, please check the ``1id-abstracts.txt'' listing contained in the Internet- Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

Mobile 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 in order 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.

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 (e.g. IP spoofing attacks), and in accordance with the IAB [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 (particularly when sends 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.

1.2. Assumptions

Mobility is constrained to a common IP address space (e.g. 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

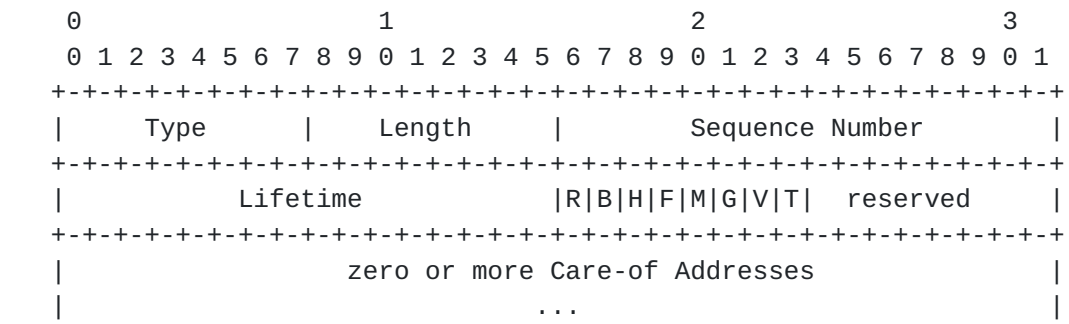
A mobile node arrives at a foreign network, listens for agent advertisements and selects a foreign agent that supports reverse tunnels. It requests this service when it registers through the selected foreign agent. At this time, and depending on how the mobile node wishes to deliver packets to the foreign 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, i.e., 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



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 two delivery styles currently supported: Direct and Encapsulating Delivery Style (section 5).

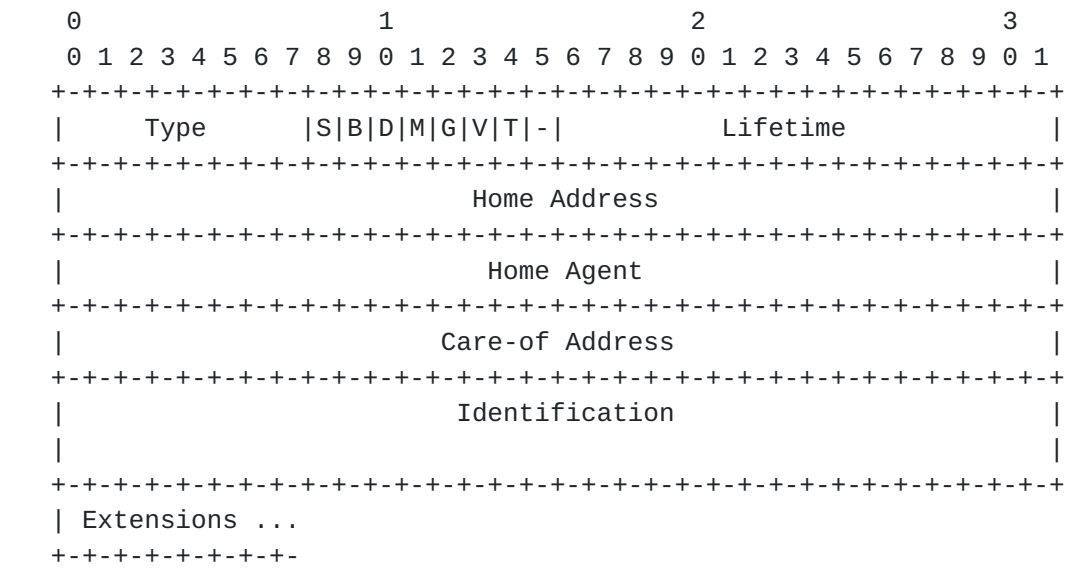
Using this information, a mobile node is able to choose a foreign agent that supports reverse tunnels. Notice that if a mobile node does not understand this bit, it simply ignores it as per [1].

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).

Most home agents would 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. Nevertheless, home agents probably already support the required decapsulation and further forwarding.

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).



The only change to the Registration Request packet is the additional 'T' bit:

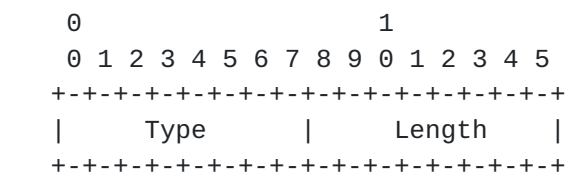
T — If the 'T' bit is set, the mobile node asks its home agent to accept a reverse tunnel from the care-of address. Mobile nodes using a foreign agent care-of address ask the foreign agent to reverse-tunnel its packets.

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 (i.e. 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 (i.e., IP in IP is assumed unless specified otherwise). For more details on the delivery styles, please refer to section 5.



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

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.

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, i.e. 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 approriate Authentication Extension (Mobile-Foreign, Foreign-Home or Mobile-Home Authentication Extension) when exchanging registration protocol datagrams. The Mobile-Home Authentication Extension MUST always be present.

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), 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 accomodate 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.

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 accomodate 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 it. For each such packet it MAY search 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.

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 Registration Request.

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 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 Registration Request.

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 (e.g. 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]. Essentialy, 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."

7. Acknowledgements

The encapsulating style of delivery was proposed by Charlie Perkins. Jim Solomon has been instrumental in shaping this document into its present form.

References

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

[2] C. Perkins. 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] D. Johnson and C. Perkins. Route Optimization in Mobile IP -- work in progress, draft-ietf-mobileip-optim-07.txt, November 1997.

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

[6] R. Atkinson. IP Authentication Header. RFC 1826, August 1995.

[7] R. Atkinson. IP Encapsulating Security Payload. RFC 1827, August 1995.

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

Editor and Chair Addresses

Questions about this document may be directed at:

Gabriel E. Montenegro
Sun Microsystems, Inc.
901 San Antonio Road
Mailstop UMPK 15-214
Mountain View, California 94303

Voice: +1-415-786-6288
Fax: +1-415-786-6445

E-Mail: gabriel.montenegro@eng.sun.com

The working group can be contacted via the current chairs:

Jim Solomon
Motorola, Inc.
1301 E. Algonquin Rd. - Rm 2240
Schaumburg, IL 60196

Voice: +1-847-576-2753
Fax: +1-847-576-3240
E-Mail: solomon@comm.mot.com

Erik Nordmark
Sun Microsystems, Inc.
901 San Antonio Road
Mailstop UMPK17-202
Mountain View, California 94303

Voice: +1-415-786-5166
E-Mail: erik.nordmark@eng.sun.com