MIP4
Internet Draft
Expires: December 2006

D. Premec
D. Damic
Siemens Mobile
June 19, 2006

Mobility Management for IPv6 Hosts using Proxy Mobile IPv4
draft-premec-mip4-ip6-proxy-mip4-00.txt

Status of this Memo

Abstract

The IPv6-based end-user device is commonly not able to utilize the advantages introduced by the mobile IP protocols. However, this specification describes how an end-user device supporting only IPv6 protocol stack may be provided with a mobility service by the mobile IPv4-based access network. The unaltered end-user device relies on the functionalities of the two network-side entities, the Home Agent

and the new Proxy Mobile Node, acting on its behalf and providing the IP layer mobility management.

Conventions used in this document

Mobile station (MS)

Mobile station is an IPv6 host that can change its point of attachment to the network. An MS does not implement the Mobile IPv6 protocol nor is it a dual stack host.

Proxy Mobile Node (PMN)

Proxy mobile node is a function implemented by the access network. Proxy mobile node performs mobile IPv4 signaling and traffic tunneling on behalf of a MS.

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 [Bra1997].

Table of Contents

1. Introduction

This specification describes how an end-user device supporting only IPv6 protocol stack may be provided with a mobility service by the mobile IPv4-based access network. The mobility management is handled completely by the network without any involvement of the end-user device.

1.1. Motivation

The operators of IPv4 networks are facing the problem of the shortage of the IPv4 address space. One possibility to cope with this problem is the introduction of NATs, but this approach is not ideal and has its own set of issues. For example, some applications exchange the IP addresses in the application layer payload. These addresses go unnoticed by the NAT and are not rewritten, with the consequence that the application fails. Such problems may be addressed by the introduction of application layer gateways at the cost of additional complexity. In this perspective, the deployment of IPv6, with its huge address space, seems very appealing.

There is also a constant growth in the number of mobile devices causing additional pressure on the already exhausted IPv4 address space. These devices expect to be able to access the network from anywhere, anytime and to provide the always-on experience. Those end-user devices also require some form of mobility management. However, most commercial operating systems available today don't provide any form of mobility support at the IP layer.

Mobile IPv4 [Per2002] as a mobility management protocol is slowly gaining momentum and operators are implementing networks based on it - there is already a significant infrastructure in the deployment supporting the mobile IPv4.

1.2. Goals

Goals of this specification are summarized below:

- To provide a network based mobility solution for IPv6 hosts
- IPv6 hosts doesn't implement whether IPv4 stack nor mobile IPv6

- Mobility management is based on mobile IPv4
- Mobility management is handled completely within the network, without the involvement of the hosts
- IPv6 service for the hosts is provided exclusively by the home network. Access network doesn't need to support IPv6 at all.

1.3. Overview of the Solution

When the access network detects an attachment of a new IPv6 device, the PMN (Proxy Mobile Node) will register the device with the HA using its own IPv4 care-of address. The IPv6 traffic of the MS will consequently be tunneled between the PMN and the HA in the IPv4 tunnel. Tunnel end points are PMN itself and the HA.

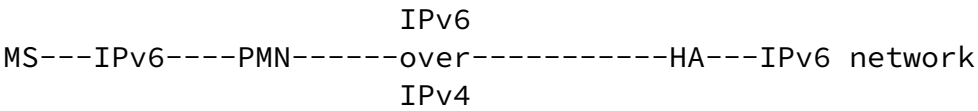


Figure 1 Deployment example

The PMN is not processing IPv6 packets in any way besides tunneling them between the HA and the MS. Thus, from the perspective of the MS, the complete access network looks like a bridge, i.e. it appears to be a single link layer connecting the MS with its HA. The MS can not tell that it is not attached to its home link - in other words, it

believes to be attached directly to the HA.

When the MS moves to the new PMN, the new PMN will register its care-of address with the HA, thus redirecting the MS traffic to itself.

1.4. Advantages

Advantages of the proposed solution are combination of advantages listed in [Tsi2006] and [Leu2006]. They are briefly summarized below:

- Mobility support for unmodified IPv6 hosts

- Leverage the existing mobile IPv4 network infrastructure, allowing the MIPv4-based access network to provide mobility service to IPv6 hosts
- Mobility management is handled completely within the network, without the involvement of the hosts
- Reduced radio link consumption: no MIP signaling over the air and no tunnel overhead over the air
- Network uses just a single mobility protocol to support both IPv4 and IPv6 hosts (protection of investment and reduction of operating costs)

2. Operation

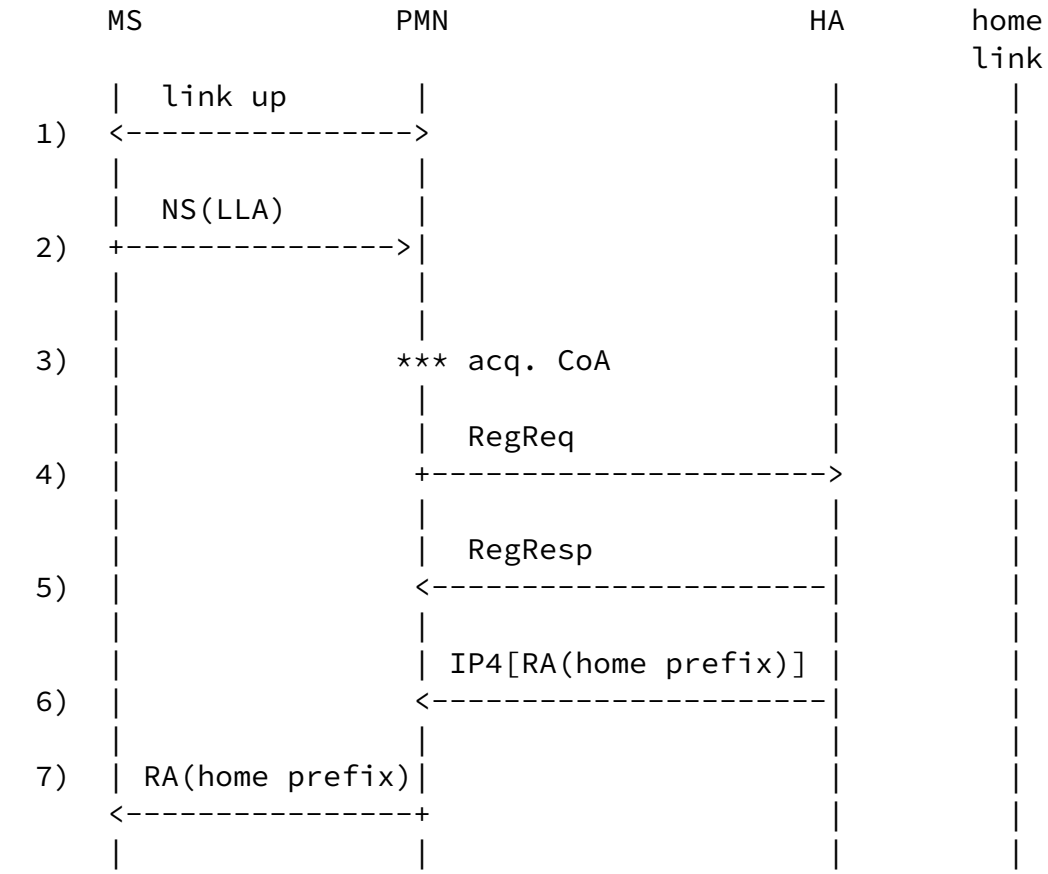
We assume a mobile IPv4-based access network. This access network is connected to the router on the home network acting as a MIPv4 HA. The HA is a dual stack node and is also acting as a default router on its IPv6 link.

We introduce a new entity which is executing mobile IPv4 procedures on behalf of the mobile node. We call this new entity a Proxy Mobile Node (PMN). The PMN resides in the access network and is located on the traffic path to the MS.

The PMN is assumed to have direct link layer connectivity (from the perspective of the IP layer) with the MS. When the MS attaches to the network, in the course of link establishment it will be authenticated. During the authentication process, the access network will learn the NAI of the MS, and the NAI must be made available to the PMN. All these actions happen at the link layer, before any IP layer connectivity.

2.1. Initial Network Entry

After the authentication and after the link layer connectivity is successfully established, the MS, being an IPv6 host, will send a Neighbor solicitation message on a newly established link to configure its link local address. The following figure illustrates the procedure in more detail:



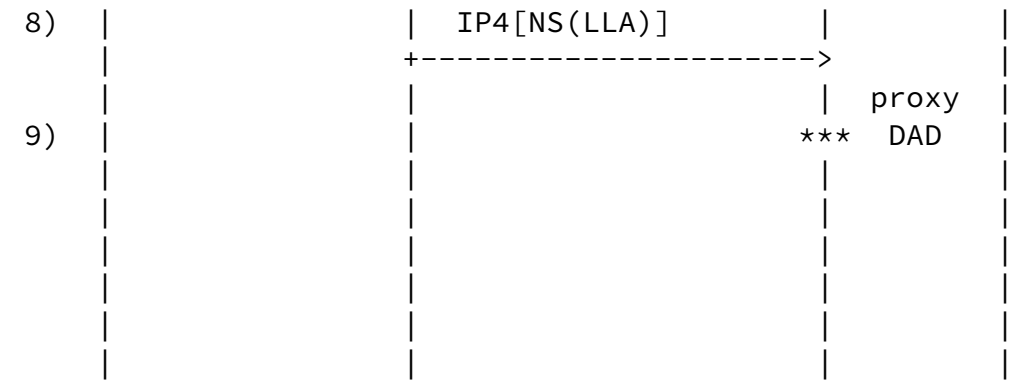


Figure 2 Initial network entry

1. In this step the link is established and the MS is authenticated. The PMN SHALL learn the NAI of the MS in this step.

2. The MS sends the Neighbor solicitation to configure its link local address.

3. When the Neighbor solicitation arrives at PMN, the PMN MAY detect that this is an IPv6 packet. This MAY trigger the PMN to register with the HA. First, the PMN MUST acquire the IPv4 address which it will use as a care-of address for the MS. How exactly the PMN acquires the IPv4 care-of address is not defined in this specification, but typically the PMN may request the address from the DHCPv4 server, or it can maintain its own address pool.

4. The PMN SHALL generate the MIPv4 Registration request using the CoA obtained in step 3 and NAI [Cal2002a] learned during the authentication. Further, the Registration request SHALL contain an IPv6 tunneling mode extension requesting the IPv6 operation mode, as defined in [Tsi2006]. The Registration request MAY also contain an IPv6 prefix extension [Tsi2006].

5. The HA SHALL create the binding between the MS, identified by its NAI, and the CoA received in the Registration request. The HA SHALL include the IPv6 code extension [Tsi2006] as a confirmation

that it supports tunneling of IPv6 traffic over MIPv4 tunnel. The code filed in the extension SHALL be set to 1 indicating that the traffic will be tunneled to the IPv4 CoA. When the PMN receives the Registration reply, it creates a binding between the newly established tunnel and the L2 link associated with the MS.

6. Immediately after sending the Registration reply, the HA SHOULD send the Router advertisement over the newly established MIPv4 tunnel. The Router advertisement is encapsulated and sent to the PMN. The inner header destination address is set to all-nodes-on-the-link address and the Router advertisement message contains the home link prefix in the prefix information option. The Router advertisement also controls which kind of address configuration the MS may use: stateless or stateful.

7. The PMN SHALL decapsulate and deliver any packets it receives via the MIPv4 tunnel directly to the MS. In this step we see the delivery of the Router advertisement sent by the HA.

8. After the MIPv4 tunnel is established, the PMN SHALL start delivering the uplink traffic to the HA. Here the Neighbor solicitation from step 2, which was delayed until the MIPv4 tunnel was set up, is tunneled to the HA.

9. The arrival of a Neighbor solicitation message verifying the tentative address SHALL trigger the HA to perform proxy DAD on behalf of the MS [Joh2004]. Having successfully performed proxy DAD, the HA SHALL deliver any traffic on the home link destined to this address via the MIPv4 tunnel to the current location of the MS. Every time the MS configures an additional IPv6 address, the HA SHALL perform proxy DAD for this additional address and bind it to the MIPv4 tunnel associated with the MS.

If the PMN is aware that the MS is an IPv6-only host, then the PMN MAY initiate the setup of the MIPv4 tunnel immediately after the link layer connection is successfully established. In other words, the step 1 in the figure above may be followed by the step 3. This has

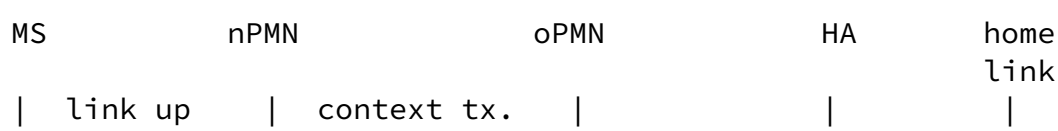
the advantage that the MIPv4 tunnel is setup in advance, before any IPv6 traffic arrives at the PMN. The benefit is that the delay caused by the tunnel setup is minimized. This is especially important because the tunnel setup delay may influence the DAD process.

It is apparent from the discussion above that the IPv6 traffic is tunneled between the PMN and the HA. Thus the whole access network appears to the MS as a single link connected directly to its HA. The MS is effectively deceived into believing that it is attached to its home link.

The MS MAY use either stateful or stateless methods to configure its home address. This specification doesn't mandate or prefer one method over another and is compatible with both methods. Important point is that whenever the MS configures an additional address, the HA SHALL perform the proxy DAD for it and add it to its binding cache.

2.2. Movement to a new PMN

The following figure describes the sequence of events when the MS moves to a new link which is associated with the new PMN.



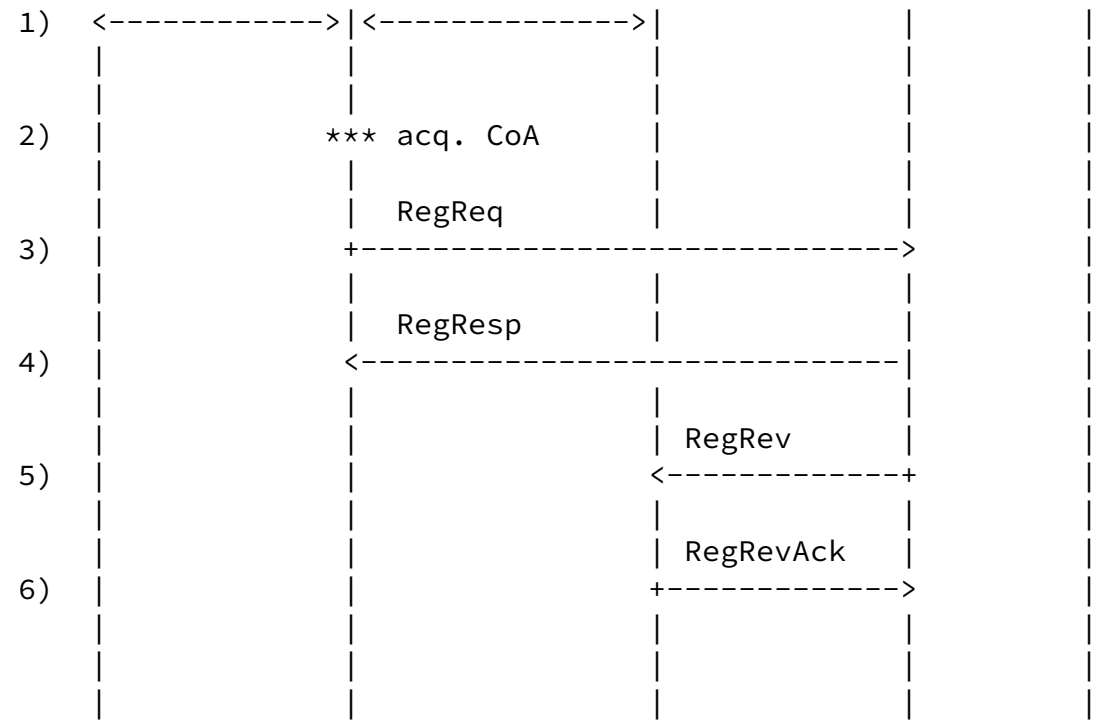


Figure 3 Movement to a new PMN

1. In this step the MS changed its point of attachment to the network. The new link layer connection with the new PMN (nPMN) is established. It is assumed that during the link layer handover the old PMN (oPMN) transfers the MS related context to the new PMN. The context SHALL include at least the NAI and the current sequence number used in MIPv4 Registration request messages. It MAY also include any packets still buffered/arriving at the oPMN. The protocol for exchanging context between PMNs is out of scope of this specification

2. - 4. These steps are the same as steps 3-5 in the section 2.1.

5. When the HA receives a Registration request for a MS for which it already has a binding cache entry, the HA SHOULD send the Registration Revoke message to the previous mobility agent, i.e.

to the oPMN. This will expedite the release of resources at the oPMN. The oPMN can safely remove all its resource associated with the PMN since it now knows that it will not receive any further traffic from the HA for this MS. The HA will perform steps 4. and 5. simultaneously.

6. The oPMN acknowledges to the HA the release of the MS related resources.

From the message flow above, it is obvious that the MS itself is not involved in the handover at all. In fact, from the perspective of the MS nothing changed, the illusion that it is connected to its home link is still being maintained by the network despite the fact that the MS actually changed its point of attachment.

2.3. Address Lifetime

Lifetime of the IPv6 address assigned to the MS and the binding lifetime held in the HA's MIPv4 context are not directly related to each other. PMN SHALL refresh the mobility binding before it expires. If the mobility binding ever expires, for whatever reason, both PMN and the HA SHALL release all resources related to that mobility binding. In case when the binding lifetime expires at the HA, the HA MAY send the Registration Revocation to the PMN, to insure that the PMN will also release its resources and that the state in both the HA and the PMN is in sync.

The MS is expected to take care of the lifetime of its IPv6 address. The HA SHALL be aware of the lifetimes of the IPv6 addresses assigned to the MS. If the MS is allowed to autoconfigure [Tho1998] its IPv6 address, then the MIPv4 binding lifetime SHALL be limited by the HA to be no more than the (remaining) lifetime of the prefix used for IPv6 address autoconfiguration. The HA MAY act as the DHCPv6 relay agent in order to learn the lifetimes of IPv6 addresses assigned by means of DHCPv6. If the IPv6 address of the MS ever expires, the HA SHALL stop defending it on the home link and SHALL remove it from its binding cache entry.

3. Home Agent Considerations

The home agent MUST support Mobile IPv4 protocol [Per2002] and the following extensions defined in [Tsi2006]: IPv6 tunneling mode extension, IPv6 code extension and IPv6 prefix extension.

Home agent is a dual stack router supporting also IPv6. The home agent MUST be configured with at least one 64-bit prefix which will serve as the home link prefix. On the interface(es) advertising the home link prefix, the HA provides the services of a default IPv6 router on the link. It also has the role of an IPv6 home agent [Joh2004]: it MUST defend home address of the MS while it is away from home, it MUST intercept its traffic and it MUST tunnel it via the MIPv4 tunnel to the current location of the MS. When the HA tunnels the packet to the PMN, the destination address of the outer header is the registered IPv4 care-of address and the source address is the HA's IPv4 address. The inner packet is the unmodified IPv6 datagram as captured on the home link.

The HA MUST provide the Mobile IPv4 service [Per2002] on at least one interface which is connected to the IPv4 network.

When the MS configures an additional IPv6 address, in order to verify its uniqueness it starts the DAD process by sending a Neighbor solicitation message to the solicited node multicast group. When the HA receives such a packet via the MIPv4 tunnel, it MUST not deliver it to the home link. Instead, the HA MUST perform proxy DAD on the home link for the address being verified. If the DAD is successful, the HA SHALL add the verified address to the binding cache entry for the MS and SHALL treat the newly configured IPv6 address as an additional home address of the MS. If the DAD process fails, the HA SHALL relay the received Neighbor advertisement to the MS via the MIPv4 tunnel.

If the MS is allowed to autoconfigure its home address, then the HA SHALL perform the proxy DAD for the home address of the MS immediately after the DAD process for the link local address of the MS is successfully over. The home address to be defended is formulated by the HA using the home link prefix and the interface identifier part of the LLA. This is because the IPv6 host is not required to verify additionally configured addresses if they are based on the same interface identifier used by the one of the already verified addresses.

The HA MAY, at its own discretion, disallow the MS from configuring and using a particular IPv6 address. When the HA receives the Neighbor solicitation message verifying the tentative address, it MAY

reply to the MS with a Neighbor advertisement packet pretending that the address being verified is already in use on the home link. This will effectively block the MS from using the tentative address.

When the HA receives the packet via the MIPv4 tunnel, it MAY check that the source IPv6 address of the inner packet is a legitimate address that the MS is allowed to use. If this is not the case, the HA SHALL discard the packet and SHALL terminate the mobility session by sending the Registration revocation to the PMN.

The HA SHALL clear the on-link determination bit in prefix information, thus preventing the MS to attempt the direct communication with the correspondent nodes having the same prefix.

The HA SHALL be aware of the address lifetime of the home address assigned to the MS. If the address lifetime expires, the HA SHALL remove the expired address from its binding cache entry.

4. Proxy Mobile Node Considerations

When the PMN detects an IPv6-only MS on the link, the PMN SHALL register the MS with the HA by sending the MIPv4 Registration request message. The Registration request message shall contain the NAI of the MS and the IPv6 tunneling mode extension as defined in [Cal2002b].

If there is no IPv6 code extension [Tsi2006] in the Registration response message or if the code value in the IPv6 code extension doesn't equal 1, the PMN SHALL not provide the MS with mobility service.

The PMN SHALL decapsulate the packets received from the HA and SHALL deliver the inner IPv6 packets to the MS. The PMN SHALL generate the appropriate link layer header and prepend it to the IPv6 packets delivered to the MS.

The PMN SHALL encapsulate the IPv6 packets received from the MS and SHALL send them to the HA via the established MIPv4 tunnel. The source address of the outer header is the registered IPv4 care-of address and the destination address is the HA's IPv4 address. The inner packet is the unmodified IPv6 datagram as received from the MS.

For the MS traffic, the PMN is acting as a link layer bridge. In particular, the PMN SHALL never decrease the hop limit field in the IPv6 header nor will it change any other field in the IPv6 header.

The PMN SHALL intercept Router advertisements sent by the HA and inspect them before relaying them to the MS. If the Router advertisement contains the source link layer address option, the PMN SHALL use the advertised link layer address as the source address when constructing the link layer header, provided that the underlying link layer technology makes use of such an address. The intercepted source LLA MAY be transferred during the handover to the new PMN as part of the MS context, and the new PMN SHOULD use the transferred link layer address when constructing the link layer header.

The PMN SHALL protect all MIPv4 signaling messages with the MN-HA authentication extension.

5. Mobile Station Considerations

Mobile station is a plain IPv6 host, and it does not have a Mobile IP stack. There are no additional requirements on the mobile station.

6. Foreign Agent Considerations

Solution described in this document supports the use of unmodified foreign agents. To the FA, the PMN will appear as regular mobile node. However, the use of FA will add an additional layer of encapsulation.

If the PMN chooses to register with the FA, the PMN will provide its IPv4 address as a care-of address and SHALL request the dynamic assignment of its home address by setting the home address field in Registration request to all zeros. The home address will be assigned by the HA in the Registration response message. The home address may be allocated from private address space and the FA may also implement the support for overlapping address spaces as described in [Leu2006].

When the PMN has an uplink packet to send, it will first encapsulate

it using the assigned IPv4 home address as the source address and the HA's IPv4 address as the destination address. Then it will deliver the encapsulated packet to the FA using either direct or encapsulated delivery style [Mon2001]. Before sending the packet to the HA, the FA will encapsulate the packet once again, using its CoA as a source address and HoA address as a destination address.

Advantage of using the non-collocated CoA mode is that the number of publicly routable IPv4 addresses is minimized: only one is needed per FA instead of one per PMN. The disadvantage is that the FA will add another layer of encapsulation when tunneling back to the HA. This adds additional processing overhead and diminishes the MTU size.

7. Security Considerations

The security considerations mentioned in [Leu2006] also apply to this specification.

According to this specification, IPv6 Neighbor discovery messages are tunneled between the MS and the HA. A number of security concerns and threats related to neighbor discovery protocol are listed in the security considerations section of [Nar1998] and in the [Nik2004]. A misbehaving MS can launch exactly the same attacks as the malicious IPv6 host physically attached to its home link (wire), but not more. In the view of the author, this specification does not introduce any new threats related to ND.

8. IANA Considerations

There are no IANA issues in this document.

9. Acknowledgments

This specification is based on the discussions and work in the WiMAX

Forum as well as the drafts [Cal2002b], [Leu2006] and [Tsi2006].

10. References

10.1. Normative References

[Ark2005] Arkko, J., Kempf, J., Zill, B., Nikander, P. "Secure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[Bra1997] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[Cal2002a]Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

[Joh2004] Johnson, D., Perkins, C., Arkko, J., "Mobility Support in IPv6", RFC 3775, June 2004

[Mon2001] Montenegro, G., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[Nar1998] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[Nik2004] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[Per2002] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[Tho1998] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998

10.2. Informative References

[Cal2002b]Calhoun, P., Engelstad P., Hiller, T., and McCann P., "IPv6 over Mobile IPv4", draft-mccann-mobileip-ipv6mipv4-03.txt, October 2002.

[Leu2006] Leung, K., Dommety, G., Yegani, P., "Mobility Management using Proxy Mobile IPv4", draft-leung-mip4-proxy-mode-00.txt, February 2006.

[Tsi2006] Tsirtsis, G., Soliman, H. and Park, V., "Dual Stack Mobile IPv4", draft-tsirtsis-v4v6-mipv4-01.txt, April 2006.

Author's Addresses

Domagoj Premec
Siemens Mobile
Heinzelova 70a
10010 Zagreb
Croatia

Phone: +385.1.610 5293
Email: domagoj.premec@siemens.com

Damjan Damic
Siemens Mobile
Heinzelova 70a
10010 Zagreb
Croatia

Phone: +385.1.633 1337
Email: damjan.damic@siemens.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.