

Network Working Group	G. Tsirtsis	
Internet-Draft	Qualcomm	
Intended status: Informational	April 16, 2009	
Expires: October 18, 2009		

[TOC](#)

Discussion of Controversial PMIP Extensions draft-tsirtsis-netext-controversy-00.txt

Status of This Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on October 18, 2009.

Abstract

This document discusses the recent controversy regarding PMIP extensions for inter-technology handoffs and multihoming. Many of the arguments presented below have been discussed in NETEXT BOF and subsequent discussions on the mailing list. They are written here in an attempt to explain why some of the proposed PMIP extensions are so controversial.

Table of Contents

- [1.](#) Requirements Notation
- [2.](#) Introduction
- [3.](#) The Internet, the Interface, and the Host
- [4.](#) What is wrong with PMIP so far
 - [4.1.](#) Signaling for Complexity
 - [4.2.](#) PMIP without Host Signaling

4.3.	PMIP and Virtual Interfaces
4.4.	PMIP and Link Layer Signaling
5.	Why extending PMIP is controversial?
5.1.	Intertech handoff, Multihoming, and Host Signaling
5.2.	PMIP with Host Signaling
5.2.1.	Historic Reasons
5.2.2.	MAG ... the new FA?
5.2.3.	Proliferation of Redundant Tools
6.	Conclusions
6.1.	Lack of Justification for PMIPv6 Extensions
6.2.	What should be done with PMIPv6
7.	Security Considerations
8.	IANA Considerations
9.	Acknowledgements
10.	Informative References

1. Requirements Notation

[TOC](#)

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 [\[RFC2119\] \(Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," March 1997.\)](#).

2. Introduction

[TOC](#)

This document discusses the recent controversy regarding PMIP extensions for inter-technology handoffs and multihoming. Many of the arguments presented below have been discussed in NETEXT BOF and subsequent discussions on the mailing list. They are written here in an attempt to explain why some of the proposed PMIP extensions are so controversial.

Following this introduction, the draft reminds readers of how interfaces and hosts are normally viewed by network layer protocols, in [Section 3 \(The Internet, the Interface, and the Host\)](#), something that is important to keep in mind while reading the rest of the document. The draft then establishes what is currently wrong with [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#), in [Section 4 \(What is wrong with PMIP so far\)](#). The draft specifically argues that:

-PMIPv6 is at best incomplete (and at worst fundamentally broken) because it relies on parameters not available to it by itself or by

any other IETF defined protocols. This affects its fundamental operation, in that:

- a) for single interface mobile nodes it is only applicable for some link layers.
- b) inter-technology handoffs are broken since the protocol does not define how a MAG/LMA knows when two different link layer technologies are somehow coupled at a given node, nor does it define how the MAG knows if a MN is reachable over a particular link layer.
- c) The narrow support for multihoming is broken since the protocol does not define how a MAG/LMA knows when handoff vs new mobility session is to be provided to the multiple interfaces.

The draft continues with outlining the controversial nature of some of the proposed PMIP extensions, in [Section 5.1 \(Intertech handoff, Multihoming, and Host Signaling\)](#). The arguments presented can be summarized as follows:

- a) To fix Inter-technology handoffs and to support multihoming properly, MN involvement is required.
- b) The MN involvement must be at the network layer (or above), and must be defined by the IETF.
- c) The need for (b) breaks the original reason for defining PMIPv6 in the IETF i.e., a mobility management protocol that does not require MN involvement.
- d) If (c) is ignored, and PMIPv6 extensions are considered then the following issues arise:
 - The definition of an MN-MAG protocol, essentially turns MAGs into FA-like entities; but FAs were designed out of MIPv6 for many reasons. Why do we need FA-like functionality back and in what form?
 - Such a protocol, would bring PMIPv6 in direct competition with MIPv6, contributing to undesirable proliferation of redundant tools in the Internet, which requires justification that is not currently available.

The fundamental question then becomes, if MN involvement is unavoidable, and if such involvement has to be at network layer, what is the justification for extending PMIPv6, when the whole premise of PMIPv6 is "no MN involvement", and when MIPv6 fully defines a protocol implementing these functions *with* MN involvement?

The draft finally concludes, in [Section 6 \(Conclusions\)](#), by first arguing that the justification for the proposed work on PMIPv6 inter-technology and multihoming support, is nonexistent and lists specific questions that need to be answered by the various factions of the NETEXT community supporting this work ([Section 6.1 \(Lack of Justification for PMIPv6 Extensions\)](#)), and by then proposes a way forward for PMIPv6 work ([Section 6.2 \(What should be done with PMIPv6\)](#)).

3. The Internet, the Interface, and the Host

[TOC](#)

This section provides some background on how "hosts" and "interfaces" are viewed in network layer specifications of the IETF. This context is important since a lot of the debate around PMIPv6 centers around the nature, availability and awareness of these entities at various places in the network e.g., MAGs according to [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) have to regularly ask the question: "Is interface X part of host Y, and associated with Interface Z (i.e., are interfaces X and Y under the same virtual interface?"

The Internet at the network layer has no notion of a host. The end points of the Internet are IP Interfaces, identified by lower layers as a link layer address (or other low layer identifier) and by the higher layers by their IP addresses. The link layer end point associated with a given interface can be presumed to be on the same or different link with other such end point interfaces, but it is mostly impossible to tell which of these link layer end points are grouped under the same interface and even harder to know which interfaces are grouped inside the same computer unit (end node or host). Several protocols do that but always at a higher layer (network or above) and always by means of explicit signaling; see more on this in [Section 4.1 \(Signaling for Complexity\)](#).

Each of the link layers on top of which IP can operate, in the end represents an interface connected to a link over which the Internet Protocol runs.

The basic IETF protocols defined for end node to access router communications (e.g., [\[RFC0792\] \(Postel, J., "Internet Control Message Protocol," September 1981.\)](#) and [\[RFC4861\] \(Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 \(IPv6\)," September 2007.\)](#)), are link-specific and treat each link layer end point on a given link, as an independent interface with no concern of whether two interfaces are part of the same node or not. For example [\[RFC4861\] \(Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 \(IPv6\)," September 2007.\)](#) says:

" Routers and multihomed hosts have multiple interfaces. The remainder of this document assumes that all sent and received Neighbor Discovery messages refer to the interface of appropriate context.... "

Indeed [\[RFC4861\]](#) (Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," September 2007.), in Appendix A, also indicates that NDP operation for multihomed nodes (on the same link) is "not straightforward". The RFC discusses various implications of same-link multihoming with respect to redirect and load-balancing functions, and places the responsibility for making this work on the end node which is the only entity that really knows what interface configuration it has. The RFC of course has nothing to say about multihomed nodes on different links, since these are in fact invisible to the network layer.

It is therefore expected that the default behavior of any access router is to treat each interface attaching to it as a distinct entity, independent from all other interfaces. This is then, one of the low level building blocks of the Internet i.e., individual, independent from each other, end-Interfaces.

On top of this low level infrastructure of interconnected end points, however, it is still possible to create more complex behaviors that are, importantly, explicitly signaled and thus, do not interfere with the fundamental operation of the Internet nor do they hinder the operation of simple nodes not equipped to handle such additional complexity.

And this is where some of the controversy around PMIP starts.

4. What is wrong with PMIP so far

[TOC](#)

This section ignores any philosophical issue, of which the author has many, against PMIP, and focuses on specific technical issues that have to do with [\[RFC5213\]](#) (Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.).

Several technical issues are identified in following subsection, after the following observations:

1) PMIP is at best incomplete (at worst fundamentally broken), because it relies on information not available by PMIP itself or any other network layer protocols defined by the IETF. This is direct result of the 'no MN involvement' assumption based on which the protocol was built resulting in not defining an MN-MAG protocol at the network layer.

2) PMIP for single interface mobiles can work for specific link layers only i.e., when the link layer used presents an identifier for the interface e.g., a MAC address, and when these links allow the MAG to explicitly identify an interface when it attaches to them.

3) PMIP's Inter-technology handoff support suffers from (1), but is also incomplete in the sense that [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) does not define when two different link layer technologies are somehow coupled at a given node (e.g., under a given virtual interface). Inter-technology handoff support breaks the 'no-MN-changes' clause of [\[RFC4830\] \(Kempf, J., "Problem Statement for Network-Based Localized Mobility Management \(NETLMM\)," April 2007.\)](#) since it requires some form of virtual interface support in the node, even if there is no MN-MAG protocol to be implemented.

4) PMIP as defined in [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) supports multihoming in a very narrow manner as defined in section 5.4 of the RFC. It requires that, if two interfaces of the same node attach to the same PMIP domain there are two options; a) the two interfaces are under the same mobility session in which case only one can be used to forward traffic to at any one time, b) the two interfaces belong to different mobility sessions, in which case they are treated as interfaces of different MNs (i.e., each has its own HoA and associated binding state in the LMA). This is good, but the PMIP protocol is again incomplete since it does not define when (a) vs (b) is supposed to happen.

4.1. Signaling for Complexity

[TOC](#)

To maintain the Internet's integrity, while allowing for arbitrarily complex behaviors, the way complexity is added on top of the rather simple IP layer is by explicit signaling of additional, more complex protocols. Here are some relevant examples:

SCTP ([\[RFC4960\] \(Stewart, R., "Stream Control Transmission Protocol," September 2007.\)](#)): binds multiple IP addresses to the same transport layer pipe between two end nodes

Mobile IP [\[RFC3344\] \(Perkins, C., "IP Mobility Support for IPv4," August 2002.\)](#), [\[RFC3775\] \(Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.\)](#): binds a stable home address to one (or more) temporary care-of addresses

What is important about these protocols is that they explicitly signal their intentions.

SCTP is signaled end to end, the routers in the path are oblivious to it, and the peer end node will accept an SCTP pipe only if it also supports SCTP. The complexity of handling multiple IP addresses as part of the same transport pipe has, therefore, no impact on any node in the Internet that does not support SCTP.

Even more relevant is the example of Mobile IP. End nodes using Mobile IP enabled nodes (Mobile Nodes, Home Agents, CNs, and Foreign Agents in MIPv4), all signal their capabilities. MNs indeed explicitly signal their desire to use Mobile IP which can be ignored or rejected automatically reverting the Mobile Node to operations (with no Mobile IP support). Thus, again, the Mobile IP family of protocols has no impact on any node that does not also support Mobile IP.

In contrast, PMIPv6 [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) operates differently. Similarly to Mobile IP it binds a stable home address to one or more temporary MAG addresses. It does that, however, without the explicit IETF-standardized involvement of the MN. The next section discusses some implications of this approach

4.2. PMIP without Host Signaling

[TOC](#)

PMIP was created under the premise of no MN involvement. The NETLMM charter (<http://www.ietf.org/html.charters/netlmm-charter.html>) clearly indicates:

"This working group is tasked with defining a network-based local mobility management protocol, where local IP mobility is handled without involvement from the mobile node."

The "no MN involvement" clause was a fundamental part of justifying the need for a new WG, since the IETF has already defined a whole family of mobility management protocol "with MN involvement", namely [\[RFC3344\] \(Perkins, C., "IP Mobility Support for IPv4," August 2002.\)](#) and [\[RFC3775\] \(Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.\)](#) with all their extensions.

Given this "no MN involvement" clause, the solution protocol, (PMIPv6) has to work within these confines resulting in the following characteristics:

PMIP and Single-Interface end nodes

A single Interface node can operate in a PMIP domain without significant problems. This is because when a single interface is attached to a PMIP domain, the end node is made to think it is essentially directly connected to the LMA. If this interface is

disconnected from one MAG and connected to another MAG, again the same illusion of direct connectivity to the LMA is preserved.

Still, this only works for link layers that present an appropriate interface identifier, e.g., a MAC address. This allows MAGs (or actually LMAs) to recognise a new link with a given MN as a link of a given node handing-off from another MAG.

PMIP and a Multi-Interface end nodes

According to [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) a PMIP MAG somehow has knowledge of whether an interface connected to it falls under one of the following categories, expressed in the form of a Handover Hint defined in section 8.4 of the RFC.

- 1: Attachment over a new interface
- 2: Handoff between two different interfaces of the mobile node
- 3: Handoff between mobile access gateways for the same interface
- 4: Handoff state unknown
- 5: Handoff state not changed (Re-registration)

Unfortunately, [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) does not say how this information is obtained. Lack of standardized signaling for the determination of this parameter is causing significant concerns. The concerns stem from the fact that this determination will most likely take place according to some proprietary solution that is not under the control of the IETF and thus, it's accuracy across multiple link layers is at best unpredictable.

PMIPv6 [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) attempts to instruct implementers to correctly set the Handoff Indication parameter but the protocol has no internal knowledge of how to set this value. For example, 3GPP has defined layer 2 procedures (and assume other link layers support the same layer 2 procedures) for the MN to indicate to the MAG the Handover Hint. This is perfectly reasonable for a body that, unlike the IETF, designs full systems and can place requirement at any layer and entity of that system. The IETF, however, has no way of ensuring that a MAG implementation will behave appropriately, independently from the Link Layer used between MN and MAG. This could easily result in incompatibilities since each SDO specific system tends to make assumptions that are not necessarily true, in the general Internet.

4.3. PMIP and Virtual Interfaces

[TOC](#)

An IP Interface is a software construct and as such can take many forms. Many IP interfaces have a one to one relationship with a physical interface e.g., an Ethernet adaptor.

Almost as often, however, IP Interfaces are virtualized in some way or another. Examples of such Virtual Interfaces are IP in IP Tunnels, VPN Tunnels, Mobile IP Interfaces, and PMIP interfaces.

All of these virtual interfaces, which are so common in IP networks are either manually configured at the relevant ends (e.g., IP in IP tunnels) or explicitly signaled by a protocols e.g., a VPN client may use IKEv2 to established an IPSEC tunnel, presenting, Mobile IP uses signaling to establish a home address to care-of address binding etc. What differentiates PMIP virtual interfaces, is that the formation of a PMIP Interface is not explicitly communicated to anyone at the network layer. It is assumed that MAGs "somehow know" whether a link layer connection from a given end node is under the same PMIP virtual interface with some other such link layer connection. This assumption, that a MAG can somehow know of the existence of a virtual interface or not, has always been a stretch and a point of contention in NETLMM WG. Again, not only the need for virtual interfaces brakes the 'no MN changes' clause of [\[RFC4830\] \(Kempf, J., "Problem Statement for Network-Based Localized Mobility Management \(NETLMM\)," April 2007.\)](#), but because of the 'no-MN-involvement' basis for PMIP, the MN can not indicate at the network layer (or above) exactly which links/interfaces relate to each other and in what way, resulting in an incomplete, non-general solution.

4.4. PMIP and Link Layer Signaling

[TOC](#)

It is true that most functions defined at the network layer can also be defined in some form or another at a lower layer. So, there is nothing technically strange or difficult about creating a link layer that supports any number of link layer protocols, which can be used to allow PMIPv6 to perform not only inter-technology handoffs, but also multihoming, flow bindings and most other functions one can build on top of a mobility protocol.

So, arguments against the idea of relying on link layers for such triggers are not about the feasibility of such an approach for a given link layer. Instead they are about how this works between all the different link layers and node configurations. For example think of an MN with several interfaces.

- IF1 and IF2 under PMIP VI1
- IF3 separate

- IF4 and IF4 under PMIP VI2

All the interfaces happen to be connected on the same PMIP domain. Say IF1 (of VI1) and IF4 (of VI2) are already connected and now one more IF is getting connected. When this new IF connects to a MAG, what information does the MAG have to know which one it is and how it relates to other IFs?

- A link layer based handover hint by itself is not enough because it does not tell the MAG whether the new IF is IF2 (associated with VI1) or IF5 (associated with VI2)
- The MNs authorization Identifier (NAI, IMSI or whatever) is clearly not enough because again it does not say whether the new IF is one of the other VI IFs (IF3, IF5) or the independent IF3.
- The L2 MAC address (if it exist) again does not provide enough information, since at best it identifies one interface and not the ones related to it.

It should be clear then that link layer signaling is not appropriate for such function since it can never provide information on other links.

5. Why extending PMIP is controversial?

[TOC](#)

5.1. Intertech handoff, Multihoming, and Host Signaling

[TOC](#)

Part of the work proposed for NETEXT WG, is about a) fixing inter-technology handoff support [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#), which as discussed earlier is broken (or at best incomplete) and b) extending PMIP to support multihoming. Multihoming in this context refers to a node with multiple interfaces (of same or different technology) connected to the Internet. These interfaces can be connected to the same or different links, access routers, or even domains. The extensions proposed would also allow for flow bindings to be used to direct different flows to different links of the same end node.

This document concludes that to really support Inter-technology handoffs and Multihoming, network layer signaling from the end node is absolutely required. The following summarizes the reasons for this conclusion.

1) Applicability for ALL link layers:

The IETF is concerned with the Internet as a whole, which operates over an ever expanding variety of link layers. Indeed mobility in the Internet means that any node can move from any link to any other link. While seamlessness of such movement is not guaranteed, the network must operate correctly and provide deterministic behaviors to the end nodes. This is why common functions, needed over different link layers, are always defined at the network layer.

2) The impossibility of global knowledge:

a) Inter-technology Handoffs:

It is not possible for a given link layer, under a given Interface, to know, and to be able to signal correctly, which other link layers and interfaces are associated with it under a PMIPv6 Virtual Interface. This is because by definition, a link layer has access only to information of its own layer. It is also not possible to have preconfigured knowledge of such relationships in the network (a.g., AAA) since the configuration of an end node can change at any time, without the AAA being notified (e.g., an device is changed or upgraded).

b) Multihoming and Flow Bindings:

The same arguments but even stronger hold in this case. If neither the link layers nor the network can not be expected to handle (a) then they can definitely not handle multihoming and flow bindings which require a lot more information regarding application mix running in the end node and instantaneous condition of different link layers available.

It should now be clear that to fix inter-technology handoff support in [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) and to extend it further to support multihoming and flow bindings, a network layer MN-MAG protocol is required.

5.2. PMIP with Host Signaling

[TOC](#)

If one concludes that host signaling is required for these advanced features, it then should be reasonable to ask:

"why host signaling is such a controversial issue for PMIP?"

Some proposals, like [draft-krishnan-netlmm-pmip-sel-00], [draft-larsson-netext-pmipv6-sma-flow-mobility-00], and even [draft-devarapalli-netext-multi-interface-support], openly talk about the need for such IETF defined signaling. At least some, however, in the NETEXT mailing list discussions present significant resistance in admitting this is necessary and the NETEXT BOF presentations were at vague and evasive on the subject.

There are several reasons for this, discussed in the following subsections.

5.2.1. Historic Reasons

[TOC](#)

The formation of NETLMM WG was strongly resisted by part of the community (see for example [draft-soliman-netlmm-harmful]). So much so that the WG's formation was even the subject of satire and sarcasm; remember NetLemmings? [draft-bombadil-netlemmings].

The group was finally formed under the assumption that it would not introduce any changes to the end nodes. Indeed the original NETLMM charter (<http://www.ietf.org/html.charters/HISTORY/netlmm-charter.2006-07-24.15.html>) said:

"...no specific mobile node to network protocol will be required for localized mobility management itself. "

The charter continued saying:

"...The (PMIPv6) protocol itself will be agnostic with respect to the last hop link layer protocol between the mobile node and the access router."

5.2.2. MAG ... the new FA?

[TOC](#)

It is not often expressed explicitly but a PMIP MAG is very similar to a MIPv4 Foreign Agent ([\[RFC3344\] \(Perkins, C., "IP Mobility Support for IPv4," August 2002.\)](#)), the main functional difference being that an [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) compliant MAG does not operate a PMIP-related protocol with the end nodes. Instead it relies on "lower layer" triggers for its operation, and suffers for that, for example by having to deal with rather complex ordering of PBUs [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#), Section 5.5.

Introduction of MN to MAG signaling at the network layer, would indeed make MAGs even more similar to MIPv4 [\[RFC3344\] \(Perkins, C., "IP Mobility Support for IPv4," August 2002.\)](#) Foreign Agents (FA). This which would raise two important issues:

During the design of MIPv6, foreign agents were considered undesirable. Based on this, FAs were designed out of the MIPv6 protocol. The PMIPv6 community has yet to make a case on why we need to re-create them now. Some of the reasons FAs are considered undesirable are:

- a) FAs required support from the Access Networks thus impeding the MN's ability to move freely without be concerned of whether or exactly what each access system supports.
- b) FAs are unnecessary in IPv6 since there is no shortage of address space (i.e., no need for shared care-of addresses in MIPv4-FA mode.
- c) FAs require a chain of trust between MNs, FAs, and HAs is increased complexity compared to the one hop association of MN-HA in MIPv6.

One could, however, make an argument for why removing FAs from this Mobile IP architecture was a mistake and we need them back in. Indeed the introduction of MAGs may point to that conclusion but this debate has never taken place in the IETF in these terms.

If the resurrection of FAs in their MAG form can be argued, however, one should also ask the question: "If we really need FA-like functionality in IPv6 mobility management, why is it not defined as part of the mainstream MIPv6 solution itself?"

- a) On one hand it is rather obvious for example, that if we incorporate MAGs into the Mobile IPv6 protocol structure, we are much more likely to have better interoperability and handoff between domains using MAGs and others that do not.
- b) On the other hand, it is not clear that any of the reasons FAs were designed out of MIPv6 are no longer valid and thus the whole endeavor is questionable.

5.2.3. Proliferation of Redundant Tools

Once the IETF developed a tool to handle a specific function e.g., Mobile IP for Mobility, the barrier for additional tools tackling the same problem space is, and should be high.

This is both reasonable and necessary to ensure wide adoption of these tools and it is the reason why it is not so easy to define a new transport protocol to replace TCP, or a new Web protocol to replace HTTP. This does not mean that a new tool is impossible, it is just a matter of having a high bar for the adoption of such redundant tools. During the formation of the NETLMM WG a case was made for basic PMIPv6, based on the idea that for a single interface mobility (i.e. intra-technology handovers), it should be possible to define a mobility management protocol that, unlike Mobile IP, does not rely on end node signaling and provides mobility transparently to the end node IP stack, without any host changes ([\[RFC4830\] \(Kempf, J., "Problem Statement for Network-Based Localized Mobility Management \(NETLMM\)," April 2007.\)](#)). As explained in detail in [Section 5.1 \(Intertech handoff, Multihoming, and Host Signaling\)](#), these initial assumptions are not possible for inter-technology handoffs and multihoming.

It should now be clear that introduction of host signaling in the PMIP protocol defeats the purpose of NETLMM/PMIP's existence since that was to provide mobility transparently to the IP stack of end nodes, unlike what MIPv6 [\[RFC3775\] \(Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.\)](#) provides based on host signaling.

6. Conclusions

[TOC](#)

6.1. Lack of Justification for PMIPv6 Extensions

[TOC](#)

During the NETEXT BOF and subsequent discussions on the mailing list a lot of time has been expending around the justification arguments for enhancing PMIPv6 further with inter-technology and multihoming features. [draft-jeyatharan-netext-multihoming-ps-01] attempts to capture such justification but it falls short in the following respects.

As discussed earlier, the NETLMM WG was established and PMIPv6 protocol was defined based on the "no MN involvement" assumption. The "no MN involvement" assumption restricts the operation of this protocol, and makes advanced features like multihoming and flow movement seem unreasonable in the context of such restrictions.

Some in the NETEXT community argue that any required MN involvement can be done at lower layers. This part of the community has to address the following issues:

- It is a well understood fact that this is not possible for all link layers. It is actually not clear at all which link layers have such capability and whether the triggers are compatible or equivalent between different technologies.
- It is important for the integrity of the Internet, that the IETF defines standardized mechanisms providing all the necessary parameters for its own protocols to operate. The author is not aware of any IETF protocol that this is not currently true. This does not seem possible when a protocol depends on external triggers not controlled by any other IETF protocol.

There are at least some in the NETEXT community, however, who recognize that MN involvement at the network layer is necessary to make these advanced features work with PMIPv6. This part of the community has to address a different set of issues.

- The definition of an MN-MAG network layer protocol, invalidates the main reason why PMIPv6 was created in the first place (i.e., mobility management with no MN involvement). It was always assumed that MIPv6 would then handle any advance functions that require MN involvement. What is the justification for changing this assumption?

As a conclusion the discussion so far comes down to one point. What is the justification for extending PMIPv6's inter-technology and multihoming capabilities? What is missing from the IETF arsenal of tools to handle such features? Why are existing tools not sufficient? These are fundamental questions that MUST be answered before any such work can be taken on.

6.2. What should be done with PMIPv6

[TOC](#)

A number of extensions proposed in the context for NETEXT WG are natural to this work and at the time of writing were approved as part of NETEXT WG Charter, e.g., Bulk Registrations, LMA Redirection etc. These tasks should indeed go ahead.

It is the opinion of this author, however, that PMIPv6 and all its extensions should be limited to single interface operations, without any inter-technology handoff and without multihoming support beyond what is already defined in [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#).

This document actually explains in earlier sections and in detail that [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) includes a number of features that are incomplete or even broken due to lack of MN-MAG protocol. [\[RFC5213\] \(Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6," August 2008.\)](#) should therefore be revised, not to add to these features, but to either change them, so no MN involvement is required, or to remove them from the RFC altogether.

7. Security Considerations

[TOC](#)

This document does not introduce any Security Considerations

8. IANA Considerations

[TOC](#)

This document does not introduce any IANA Considerations

9. Acknowledgements

[TOC](#)

Thanks to Marcelo Bagnulo who poked a number of holes on my original arguments causing me significant pain :-), but in the end helping me refine and clarify them significantly. Also thanks to Gerardo Giaretta and Hesham Soliman for useful comments and suggestions. Many of the arguments presented below are not solely mine but have been discussed in the past in NETLMM WG mailing list, and more recently in NETEXT BOF and subsequent discussions on the mailing list.

10. Informative References

[TOC](#)

[RFC0792]	Postel, J., " Internet Control Message Protocol ," STD 5, RFC 792, September 1981 (TXT).
[RFC0894]	Hornig, C., " Standard for the transmission of IP datagrams over Ethernet networks ," STD 41, RFC 894, April 1984 (TXT).
[RFC2004]	Perkins, C. , " Minimal Encapsulation within IP ," RFC 2004, October 1996 (TXT , HTML , XML).
[RFC2119]	

	Bradner, S. , " Key words for use in RFCs to Indicate Requirement Levels ," BCP 14, RFC 2119, March 1997 (TXT , HTML , XML).
[RFC2225]	Laubach, M. and J. Halpern , " Classical IP and ARP over ATM ," RFC 2225, April 1998 (TXT , HTML , XML).
[RFC3344]	Perkins, C., " IP Mobility Support for IPv4 ," RFC 3344, August 2002 (TXT).
[RFC3775]	Johnson, D., Perkins, C., and J. Arkko, " Mobility Support in IPv6 ," RFC 3775, June 2004 (TXT).
[RFC4830]	Kempf, J., " Problem Statement for Network-Based Localized Mobility Management (NETLMM) ," RFC 4830, April 2007 (TXT).
[RFC4861]	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, " Neighbor Discovery for IP version 6 (IPv6) ," RFC 4861, September 2007 (TXT).
[RFC4960]	Stewart, R., " Stream Control Transmission Protocol ," RFC 4960, September 2007 (TXT).
[RFC5213]	Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, " Proxy Mobile IPv6 ," RFC 5213, August 2008 (TXT).
[RFC5226]	Narten, T. and H. Alvestrand, " Guidelines for Writing an IANA Considerations Section in RFCs ," BCP 26, RFC 5226, May 2008 (TXT).

Author's Address

[TOC](#)

	George Tsirtsis
	Qualcomm
EMail:	tsirtsis@gmail.com

Full Copyright Statement

[TOC](#)

Copyright © The IETF Trust (2009).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

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.