

NETEXT WG  
Internet-Draft  
Intended status: Informational  
Expires: September 14, 2016

T. Melia, Ed.  
Kudelski Security  
S. Gundavelli, Ed.  
Cisco  
March 13, 2016

Logical-interface Support for Multi-access enabled IP Hosts  
draft-ietf-netext-logical-interface-support-14

Abstract

A Logical-interface is a software semantic internal to the host operating system. This semantic is available in all popular operating systems and is used in various protocol implementations. The Logical-interface support is required on the mobile node attached to a Proxy Mobile IPv6 domain, for leveraging various network-based mobility management features such as inter-technology handoffs, multihoming and flow mobility support. This document explains the operational details of Logical-interface construct and the specifics on how the link-layer implementations hide the physical interfaces from the IP stack and from the network nodes on the attached access networks. Furthermore, this document identifies the applicability of this approach to various link-layer technologies and analyzes the issues around it when used in conjunction with various mobility management features.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on September 14, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	4
3. Hiding Link-layer Technologies - Approaches and Applicability . . . . .	5
3.1. Link-layer Abstraction - Approaches . . . . .	5
3.2. Link layer support . . . . .	6
3.3. Logical Interface . . . . .	6
4. Technology Use cases . . . . .	7
5. Logical Interface Functional Details . . . . .	8
5.1. Configuration of a Logical Interface . . . . .	9
5.2. Logical-Interface Forwarding Table . . . . .	9
6. Logical Interface Use-cases in Proxy Mobile IPv6 . . . . .	11
6.1. Multihoming Support . . . . .	11
6.2. Inter-Technology Handoff Support . . . . .	12
6.3. Flow Mobility Support . . . . .	13
7. IANA Considerations . . . . .	14
8. Security Considerations . . . . .	15
9. Authors . . . . .	16
10. Acknowledgements . . . . .	16
11. References . . . . .	17
11.1. Normative References . . . . .	17
11.2. Informative References . . . . .	17
Authors' Addresses . . . . .	18

## 1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] is a network-based mobility management protocol standardized by IETF. One of the key goals of the PMIPv6 protocol is to enable a mobile node to perform handovers across access-networks based on different access technologies. The protocol was also designed with the goal to allow a mobile node to simultaneously attach to different access networks and perform flow-based access selection [I-D.ietf-netext-pmipv6-flowmob]. The base protocol features specified in [RFC5213] and [RFC5844] has support for these capabilities. However, for supporting these features, the mobile node is required to be enabled with specific software configuration known as logical-interface support. The logical-interface configuration is essential for a mobile node to perform inter-access handovers without impacting the IP sessions on the host.

A Logical Interface construct is internal to the operating system. It is an approach of interface abstraction, where a logical link-layer implementation hides a variety of physical interfaces from the IP stack. This semantic was used on a variety of operating systems to implement applications such as Mobile IP client [RFC6275] and IPsec VPN client [RFC4301]. Many host operating systems have support for some form of such logical interface construct. But, there is no specification which documents the behavior of these logical-interface, or the requirements of a logical interface for supporting the above mentioned mobility management features. This specification attempts to document these aspects.

The rest of the document provides a functional description of a Logical Interface on the mobile node and the interworking between a mobile node using a logical interface and the network elements in the Proxy Mobile IPv6 domain. It also analyzes the issues involved with the use of logical-interface and characterizes the contexts in which such usage is appropriate.

## 2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in Proxy Mobile IPv6 specifications, [RFC5213] and [RFC5844]. In addition, this document uses the following terms:

PIF (Physical Interface) - It is a network interface module on the host that is used for connecting to an access network. An host typically has number of network interface modules, such as Ethernet, Wireless LAN, LTE ..etc. Each of these network interfaces can support specific link technology.

LIF (Logical Interface) - It is a virtual interface in the IP stack. Logical interface appears to the IP stack just as any other physical interface, provides similar semantics with respect to packet transmit and receive functions to the upper layers of the IP stack. However, it is only a logical construct and is not a representation of an instance of any physical hardware.

SIF (Sub Interface) - It is a physical or logical interface that is part of a logical interface construct. For example, a logical interface may have been created abstracting two physical interfaces, LTE and WLAN. These physical interfaces, LTE and WLAN are referred to as sub-interfaces of that logical interface. In some cases, a sub-interface can also be another logical interface, such as an IPsec tunnel interface.

### 3. Hiding Link-layer Technologies - Approaches and Applicability

There are several techniques that allow hiding of changes in access-technology changes from the host layer. These changes in access technology is primarily due to host's movement between access networks. This section classifies these existing techniques into a set of generic approaches, according to their most representative characteristics. Later sections of this document analyze the applicability of these solution approaches for supporting features such as, inter-technology handovers and IP flow mobility support for a mobile node.

#### 3.1. Link-layer Abstraction - Approaches

The following generic mechanisms can hide access technology changes from host IP layer:

- o Link-layer Support - Certain link-layer technologies are able to hide physical media changes from the upper layers. For example, IEEE 802.11 is able to seamlessly change between IEEE 802.11a/b/g physical layers. Also, an 802.11 STA can move between different Access Points within the same domain without the IP stack being aware of the movement. In this case, the IEEE 802.11 MAC layer takes care of the mobility, making the media change invisible to the upper layers. Another example is IEEE 802.3, that supports changing the rate from 10Mbps to 100Mbps and to 1000Mbps. Another example is the situation in the 3GPP Evolved Packet System [TS23401] where a UE can perform inter-access handovers between three different access technologies (2G GERAN, 3G UTRAN, and 4G E-UTRAN) that are invisible to the IP layer at the UE.
- o A logical interface denotes a mechanism that logically groups several physical interfaces so they appear to the IP layer as a single interface (see Figure 1). Depending on the type of access technologies, it might be possible to use more than one physical interface at a time -- such that the node is simultaneously attached via different access technologies -- or just to perform handovers across a variety of physical interfaces. Controlling the way the different access technologies are used (simultaneous, sequential attachment, etc) is not trivial and requires additional intelligence and/or configuration within the logical interface implementation. The configuration is typically handled via a connection manager, and based on a combination of user preferences on one hand, and operator preferences such as those provisioned by the Access Network Discovery and Selection Function (ANDSF) [TS23402] on the other hand. The IETF Interfaces MIB specified in [RFC2863] and the YANG data model for Interface management specified in [RFC7223] treats logical interface as just any other

type of network interface on the host. This essentially makes logical interface as a natural operating system construct.

### 3.2. Link layer support

Link layer mobility support applies to cases when the same link layer technology is used and mobility can be fully handled at that layer. One example is the case where several 802.11 access points are deployed in the same subnet with a common IP layer configuration (DHCP server, default router, etc.). In this case the handover across access points need not to be hidden to the IP layer since the IP layer configuration remains the same after a handover. This type of scenario is applicable to cases when the different points of attachment (i.e. access points) belong to the same network domain, e.g. Enterprise, hotspots from same operator, etc.

Since this type of link layer technology does not typically allow for simultaneous attachment to different access networks of the same technology, the logical interface would not be used to provide simultaneous access for purposes of multihoming or flow mobility. Instead, the logical interface can be used to provide inter-access technology handover between this type of link layer technology and another link layer technology, e.g., between IEEE 802.11 and IEEE 802.16.

### 3.3. Logical Interface

The use of a logical interface allows the mobile node to provide a single interface perspective to the IP layer and its upper layers (transport and application). Doing so allows to hide inter-access technology handovers or application flow handovers across different physical interfaces.

The logical interface may support simultaneous attachment, in addition to sequential attachment. It requires additional support at the node and the network in order to benefit from simultaneous attachment. For example special mechanisms are required to enable addressing a particular interface from the network (e.g. for flow mobility). In particular extensions to PMIPv6 are required in order to enable the network (i.e., the MAG and LMA) to deal with logical interface, instead to IP interfaces as current RFC5213 does. RFC5213 assumes that each physical interface capable of attaching to a MAG is an IP interface, while the logical interface solution groups several physical interfaces under the same IP logical interface.

It is therefore clear that the Logical Interface approach satisfies the multi technology and the sequential vs: simultaneous access support.

#### 4. Technology Use cases

3GPP has defined the Evolved Packet System (EPS) for heterogeneous wireless access. A mobile device equipped with 3GPP and non-3GPP wireless technologies can simultaneously or sequentially connect any of the available devices and receive IP services through any of them. This document focuses on employing a logical interface for simultaneous and sequential use of a variety of access technologies.

As mentioned in the previous sections the Logical Interface construct is able to hide to the IP layer the specifics of each technology in the context of network based mobility (e.g. in multi-access technology networks based on PMIPv6). The LIF concept can be used with at least the following technologies: 3GPP access technologies (3G, LTE), IEEE 802.16 access technology, and IEEE 802.11 access technology.

In some UE implementations the wireless connection setup is based on creation of a PPP interface between the IP layer and the wireless modem that is configured with the IPCP and IPv6CP protocol [RFC5072]. In this case the PPP interface does not have any L2 address assigned. In some other implementations the wireless modem is presented to the IP layer as a virtual Ethernet interface.

## 5. Logical Interface Functional Details

This section identifies the functional details of a logical interface and provides some implementation considerations.

On most operating systems, a network interface is associated with a physical device that offers the services for transmitting and receiving IP packets from the network. In some configurations, a network interface can also be implemented as a logical interface which does not have the inherent capability to transmit, or receive packets on a physical medium, but relies on other physical interfaces for such services. Example of such configuration is an IP tunnel interface.

An overview of a logical interface is shown in Figure 1. The logical interface allows heterogeneous attachment while making changes in the underlying media transparent to the IP stack. Simultaneous and sequential network attachment procedures are therefore possible, enabling inter-technology and flow mobility scenarios.

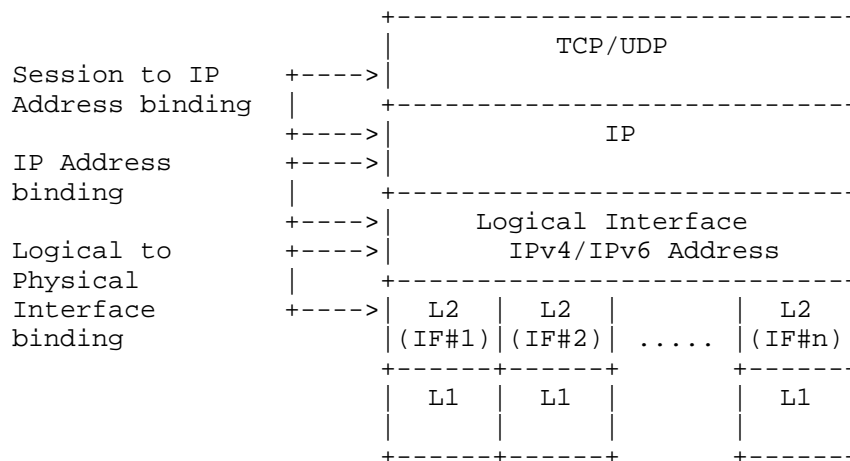


Figure 1: General overview of logical interface

From the perspective of the IP stack and the applications, a Logical interface is just another interface. In fact, the logical interface is only visible to the IP and upper layers when enabled. A host does not see any operational difference between a Logical and a physical interface. As with physical interfaces, a Logical interface is represented as a software object to which IP address configuration is bound. However, the Logical interface has some special properties which are essential for enabling inter-technology handover and flow-mobility features. Following are those properties:



1. The logical interface has a relation to a set of physical interfaces (sub-interfaces) on the host that it is abstracting. These sub-interfaces can be attached or detached from the Logical Interface at any time. The sub-interfaces attached to a Logical interface are not visible to the IP and upper layers.
2. The logical interface may be attached to multiple access technologies.
3. The Transmit/Receive functions of the logical interface are mapped to the Transmit/Receive services exposed by the sub-interfaces. This mapping is dynamic and any change is not visible to the upper layers of the IP stack.
4. The logical interface maintains IP flow information for each of its sub-interfaces. A conceptual data structure is maintained for this purpose. The host may populate this information based on tracking each of the sub-interface for the active flows.

#### 5.1. Configuration of a Logical Interface

A host may be statically configured with the logical interface configuration, or an application such as a connection manager on the host may dynamically create it. Furthermore, the set of sub-interfaces that are part of a logical interface construct may be a fixed set, or may be kept dynamic, with the sub-interfaces getting added or deleted as needed. The specific details related to these configuration aspects are implementation specific and are outside the scope of this document.

The IP layer should be configured with a default router reachable via the logical interface. The default router can be internal to the logical interface, i.e., it is a logical router that in turns decide which physical interface is to be used to transmit packets.

#### 5.2. Logical-Interface Forwarding Table

The logical interface maintains the list of sub-interfaces that are part of logical-interface construct. This is a conceptual data structure, called as the Logical-Interface Forwarding Table.

The logical interface also maintains the list of flows associated with a given sub-interface and this conceptual data structure is called as the PIF Table. Both of these data structures have to be associated with a logical interface, and are depicted in Figure 2.

LIF TABLE		FLOW table	
PIF_ID	FLOW Routing Policies	FLOW ID	Physical_Intf_Id
	Link Status		
PIF_ID	FLOW Routing Policies	FLOW_ID	Physical_Intf_Id
	Link Status		
....	....	....	....

Figure 2: Logical Interface Table

The LIF table maintains the mapping between the LIF and each PIF associated to the LIF (refer to property #3, Figure 1). For each PIF entry the table should store the associated Routing Policies, and the Link Status of the PIF (e.g. active, not active). The method by which the Routing Policies are configured on the host is out of scope for this document.

The FLOW table allows the logical interface to properly route each IP flow over the right interface. The logical interface can identify the flows arriving on its sub-interfaces and associate them to those sub-interfaces. This approach is similar to reflective QoS performed by the IP routers. For locally generated traffic (e.g. unicast flows), the logical interface should perform interface selection based on the Flow Routing Policies. In case traffic of an existing flow is suddenly received from the network on a different sub-interface than the one locally stored, the logical interface should interpret the event as an explicit flow mobility trigger from the network and it should update the PIF\_ID parameter in the FLOW table. Similarly, locally generated events from the sub-interfaces, or configuration updates to the local policy rules can cause updates to the table and hence trigger flow mobility.

## 6. Logical Interface Use-cases in Proxy Mobile IPv6

This section explains how the Logical interface support on the mobile node can be used for enabling some of the Proxy Mobile IPv6 protocol features.

### 6.1. Multihoming Support

A mobile node with multiple interfaces can attach simultaneously to the Proxy Mobile IPv6 domain. If the host is configured to use Logical interface over the physical interfaces through which it is attached, following are the related considerations.

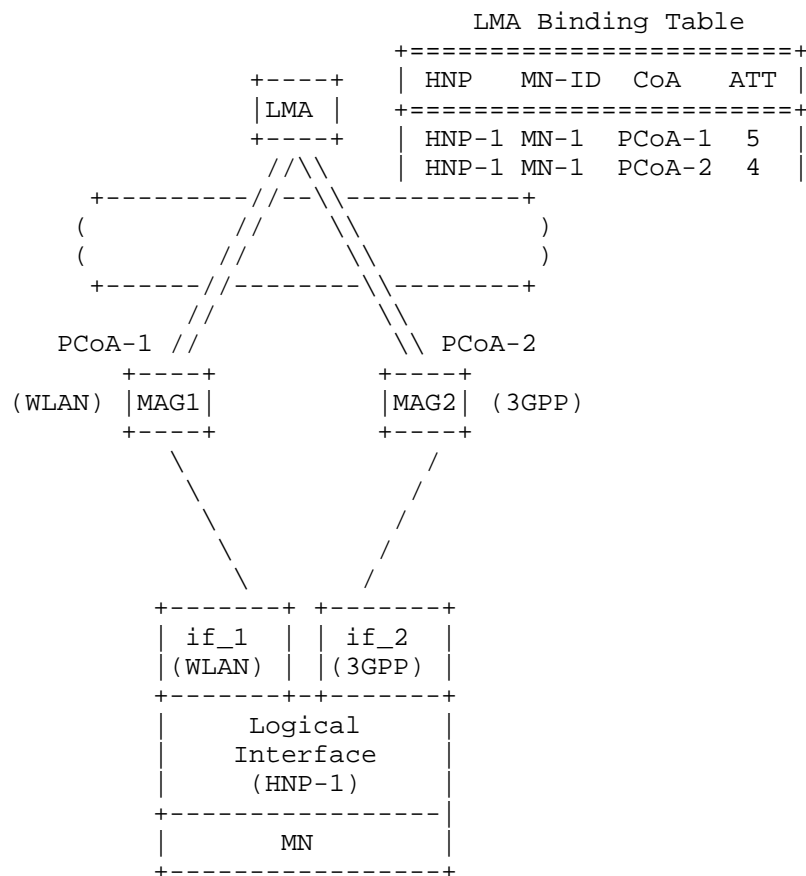


Figure 3: Multihoming Support

## 6.2. Inter-Technology Handoff Support

The Proxy Mobile IPv6 protocol enables a mobile node with multiple network interfaces to move between access technologies, but still retaining the same address configuration on its attached interface. The protocol enables a mobile node to achieve address continuity during handoffs. If the host is configured to use Logical interface over the physical interface through which it is attached, following are the related considerations.

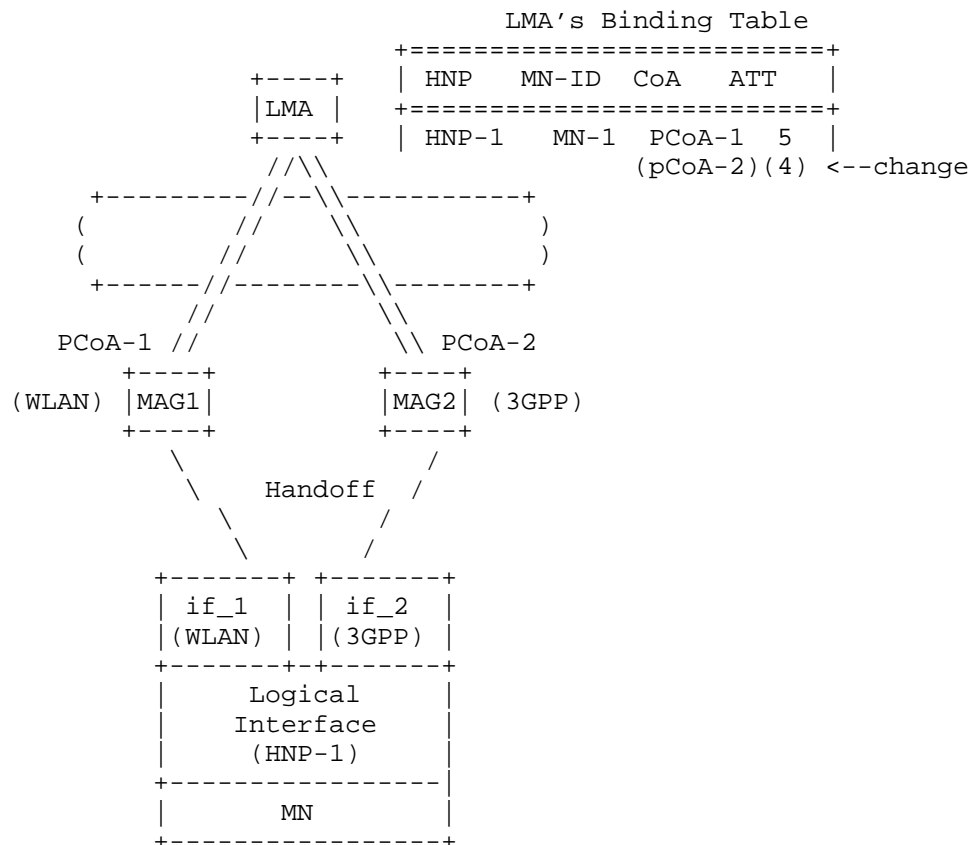


Figure 4: Inter-Technology Handoff Support

- o When the mobile node performs an handoff between if\_1 and if\_2, the change will not be visible to the applications of the mobile node.

- o The protocol signaling between the network elements will ensure the local mobility anchor will switch the forwarding for the advertised prefix set from MAG1 to MAG2.

### 6.3. Flow Mobility Support

For supporting IP flow mobility, there is a need to support vertical handoff scenarios such as transferring a subset of prefix(es) (hence the flows associated to it/them) from one interface to another. The mobile node can support this scenario by using the Logical interface support. This scenario is similar to the Inter- technology handoff scenario defined in Section 6.2, only a subset of the prefixes are moved between interfaces.

Additionally, IP flow mobility in general initiates when the LMA decides to move a particular flow from its default path to a different one. The LMA can decide on which is the best MAG that should be used to forward a particular flow when the flow is initiated e.g. based on application policy profiles) and/or during the lifetime of the flow upon receiving a network-based or a mobile-based trigger. However, the specific details on how the LMA can formulate such flow policy is outside the scope of this document.

## 7. IANA Considerations

This specification does not require any IANA Actions.

## 8. Security Considerations

This specification explains the operational details of Logical interface on an IP host. The Logical Interface implementation on the host is not visible to the network and does not require any special security considerations.

Different layer-2 interfaces and the access networks to which they are connected have different security properties. For example, the layer-2 network security of an end-user operated Wireless LAN network is in the control of the home user and whereas an LTE operator has the control on the layer-2 security of the LTE access network. An external entity using lawful means, or through other means obtain the security keys from the LTE operator and the same may not be possible in the case of a home user operated wireless LAN network. Therefore, grouping interfaces with such varying security properties into one logical interface could have negative consequences in some cases. Such differences though subtle, are entirely hidden by logical interfaces and are unknown to the upper layers.

## 9. Authors

This document reflects contributions from the following authors (listed in alphabetical order):

Carlos Jesus Bernardos Cano

cjbc@it.uc3m.es

Antonio De la Oliva

aoliva@it.uc3m.es

Yong-Geun Hong

yonggeun.hong@gmail.com

Kent Leung

kleung@cisco.com

Tran Minh Trung

trungtm2909@gmail.com

Hidetoshi Yokota

yokota@kddilabs.jp

Juan Carlos Zuniga

JuanCarlos.Zuniga@InterDigital.com

## 10. Acknowledgements

The authors would like to acknowledge all the discussions on this topic in NETLMM and NETEXT working groups. The authors would also like to thank Joo-Sang Youn, Pierrick Seite, Rajeev Koodli, Basavaraj Patil, Peter McCann, Julien Laganier, Maximilian Riegel, Georgios karagian, Stephen Farrell, Benoit Claise for their inputs to the document.

## 11. References



## 11.1. Normative References

- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<http://www.rfc-editor.org/info/rfc5213>>.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, DOI 10.17487/RFC5844, May 2010, <<http://www.rfc-editor.org/info/rfc5844>>.

## 11.2. Informative References

- [I-D.ietf-netext-pmipv6-flowmob] Bernardos, C., "Proxy Mobile IPv6 Extensions to Support Flow Mobility", draft-ietf-netext-pmipv6-flowmob-17 (work in progress), March 2016.
- [RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000, <<http://www.rfc-editor.org/info/rfc2863>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <<http://www.rfc-editor.org/info/rfc4301>>.
- [RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, DOI 10.17487/RFC5072, September 2007, <<http://www.rfc-editor.org/info/rfc5072>>.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <<http://www.rfc-editor.org/info/rfc6275>>.
- [RFC7223] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 7223, DOI 10.17487/RFC7223, May 2014, <<http://www.rfc-editor.org/info/rfc7223>>.
- [TS23401] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.", 2009.
- [TS23402] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture Enhancements for non-3GPP Accesses.", 2009.

Authors' Addresses

Telemaco Melia (editor)  
Kudelski Security  
Geneva  
Switzerland

Email: telemaco.melia@gmail.com

Sri Gundavelli (editor)  
Cisco  
170 West Tasman Drive  
San Jose, CA 95134  
USA

Email: sgundave@cisco.com



NETEXT WG  
Internet-Draft  
Intended status: Standards Track  
Expires: June 21, 2014

X. Zhou  
ZTE Corporation  
J. Korhonen  
Broadcom  
C. Williams  
Consultant  
S. Gundavelli  
Cisco  
CJ. Bernardos  
UC3M  
December 18, 2013

Prefix Delegation Support for Proxy Mobile IPv6  
draft-ietf-netext-pd-pmip-14

Abstract

This specification defines extensions to the Proxy Mobile IPv6 protocol for allowing a mobile router in a Proxy Mobile IPv6 domain to obtain IP prefixes for its attached mobile networks using DHCPv6 prefix delegation. Network-based mobility management support is provided for those delegated IP prefixes just as it is provided for the mobile node's home address. Even if the mobile router performs a handoff and changes its network point of attachment, mobility support is ensured for all the delegated IP prefixes and for all the IP nodes in the mobile network that use IP address configuration from those delegated IP prefixes.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on June 21, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	4
2. Terminology . . . . .	6
3. Solution Overview . . . . .	7
3.1. Stated Assumptions . . . . .	7
3.2. Deployment Models . . . . .	8
3.2.1. Delegating Router co-located with Mobile Access Gateway . . . . .	8
3.2.2. Delegating Router co-located with Local Mobility Anchor . . . . .	9
3.2.3. Static Configuration of Delegated Mobile Network Prefixes . . . . .	11
4. Message formats . . . . .	12
4.1. Delegated Mobile Network Prefix Option . . . . .	12
4.2. Status Codes . . . . .	14
5. Operational Details . . . . .	14
5.1. MAG Considerations . . . . .	14
5.1.1. Extension to Binding Update List Entry Data Structure . . . . .	14
5.1.2. Signaling Considerations . . . . .	14
5.1.3. DHCP - MAG Interactions . . . . .	16
5.1.3.1. Delegating Router co-located with Mobile Access Gateway . . . . .	16
5.1.3.2. Delegating Router co-located with Local Mobility Anchor . . . . .	18
5.1.4. Packet Forwarding . . . . .	19
5.2. LMA Considerations . . . . .	20
5.2.1. Extensions to Binding Cache Entry Data Structure . . . . .	20
5.2.2. Signaling Considerations . . . . .	20
5.2.3. Packet Forwarding . . . . .	22
5.3. Security Policy Database (SPD) Example Entries . . . . .	22
6. Security Considerations . . . . .	23
7. IANA Considerations . . . . .	24

8. Acknowledgments . . . . .	24
9. References . . . . .	25
9.1. Normative References . . . . .	25
9.2. Informative References . . . . .	25
Authors' Addresses . . . . .	26

## 1. Introduction

Proxy Mobile IPv6 [RFC5213] enables network-based mobility management support for an IP host without requiring its participation in any IP mobility signaling. In Proxy Mobile IPv6 (PMIPv6), the mobile access gateway (MAG) performs the mobility management function on behalf of the mobile node (MN). The local mobility anchor (LMA) is the home agent for the MN and the topological anchor point. The mobility elements (LMA and MAGs) in the network allow an IP host to obtain an IPv4 address and/or a set of IPv6 addresses and be able to obtain IP mobility support for those IP address(es) within the Proxy Mobile IPv6 domain. In this context, the mobility management support is enabled for an individual IP host, which is the mobile node. The IPv4 home address, or the IPv6 home network prefixes are logically bound to the link shared between the mobile access gateway and the mobile node and only the mobile node can use those IP address(es) by configuring them on the interface attached to that link. Currently, there is no mobility support for the mobile networks attached to a mobile router in a Proxy Mobile IPv6 domain.

This specification defines extensions to the Proxy Mobile IPv6 protocol (a new mobility option for carrying delegated prefix information in proxy binding update and proxy binding acknowledgement messages) for allowing mobility support to the mobile networks attached to a mobile router. The mobile router can request the mobility entities in the Proxy Mobile IPv6 domain for one or more delegated IP prefixes using DHCP Prefix Delegation extensions [RFC3633], or through other means such as static configuration, or access technology specific mechanisms. The mobility entities in the PMIPv6 network provide network-based mobility management support for those delegated prefixes just as it is supported for a home address. The delegated prefixes are hosted in the mobile network attached to the mobile router. IP mobility is ensured for all the IP nodes in the mobile network, even as the mobile router performs a handoff by changing its point of network attachment within the Proxy Mobile IPv6 domain. The local mobility anchor in the Proxy Mobile IPv6 domain will not track the individual IP sessions for all the IP nodes in the mobile network, it only tracks a single mobile router session that is hosting the mobile network and associates the delegated IP prefixes with that session. Although the protocol solution defined in this specification also allows signaling IPv4 subnets between the mobile access gateway and the local mobility anchor, the delegation of IPv4 subnets to the mobile router is out of scope of this specification.

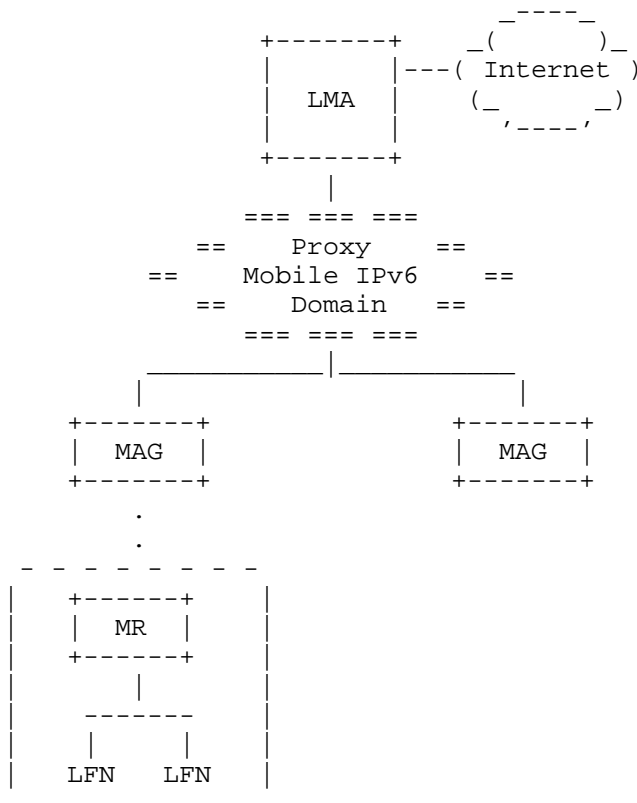


Figure 1: Mobile Router in Proxy Mobile IPv6 Domain

Within the context of this document, the definition of a mobile router extends that of a mobile node definition from [RFC5213], by adding routing capability between the mobile network and the point of attachment of the mobile router. The network of nodes part of the mobile network are referred to as locally fixed nodes (LFN) and they all move with the mobile router as a single cluster. As the mobile router moves, the LFNs are not aware of the mobility of the MR to a new point of attachment. Figure 1 illustrates a mobile router in a Proxy Mobile IPv6 domain.

The rest of the document identifies the protocol extensions and the operational details of the local mobility anchor and mobile access gateway for supporting this specification.



## 2. Terminology

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].

All the mobility related terms used in this document are to be interpreted as defined in Proxy Mobile IPv6 specifications [RFC5213] and [RFC5844]. All the DHCP related terms are to be interpreted as defined in DHCPv6-PD for NEMO [RFC6276], DHCPv6-PD [RFC3633] and Subnet Allocation Option for DHCPv4 [RFC6656]. This document also provides a context-specific explanation to the following terms used in this document, and originally defined in the Mobile Network terminology document [RFC4885].

### Mobile Router (MR)

The term mobile router is used to refer to an IP router whose mobility is managed by the network while being attached to a Proxy Mobile IPv6 domain. The mobile router is a mobile node as defined in [RFC5213], but with additional capabilities for supporting an attached mobile network. The MR's interface used for attachment to the mobile access gateway is referred to as the egress interface. Any MR's interface used for attachment to the mobile network is referred to as ingress interface. The mobility entities in the Proxy Mobile IPv6 domain provide mobility for the IPv4/IPv6 address(es) assigned to the mobile node's egress link and also mobility support to the network prefixes hosted in the network attached to the mobile router.

### Mobile Network

It is an IP network attached to a mobile router. There can be many IP nodes in this IP network. The mobile router is a gateway for these IP nodes for reaching other IP networks or the Internet. The mobile router and the attached IP networks move as a single cluster.

### Delegated Mobile Network Prefix (DMNP)

The Delegated Mobile Network Prefix is an IPv4/IPv6 prefix delegated to a mobile router and is hosted in the mobile network. The IP nodes in the mobile network will be able to obtain IP address configuration from the delegated mobile network prefix and will have IP mobility support for that address configuration. The DMNP is topologically anchored on the local mobility anchor and the mobility elements in the Proxy Mobile IPv6 domain provide IP mobility support for the prefix, by forwarding the mobile network

traffic to the mobile router.

#### Locally Fixed Node (LFN)

A Locally Fixed Node is an IP node in the mobile network. As the mobile router performs a handoff and changes its network point of attachment, the locally fixed node moves along with the mobile router.

### 3. Solution Overview

This section provides an overview of the operation of this specification, as well as lists the stated assumptions. This specification references three different deployment scenarios and explains the protocol operation.

#### 3.1. Stated Assumptions

- o The mobile router is a mobile node as defined in [RFC5213], but with additional capabilities for routing IP packets between its egress interface (interface used for attachment to the mobile access gateway) and any of its ingress interfaces (interface used for attachment to the mobile network).
- o The specification assumes that a mobile router is an IPv4 and/or IPv6 router without any capability for mobility management.
- o The mobile router can obtain the delegated IP prefix(es) for its attached mobile networks using DHCPv6 Prefix Delegation, Static configuration, or through mechanisms specific to the access technology. This document assumes DHCPv6 Prefix Delegation [RFC3633] and in conjunction with the Prefix Exclude Option [RFC6603] as the default mechanism for prefix assignment to the mobile node. It defines an interworking between the mobility entities and the DHCPv6 functional elements in a non-normative way. The mechanism how to delegate IPv4 subnets to a mobile router is out of scope of this specification.
- o The mobile router obtains the IP address configuration for its egress roaming interface as specified in [RFC5213] and [RFC5844]. The mobile router along with its mobile networks will be able to perform handoff and change its point of attachment in the network and will be able to retain IP mobility support.
- o When using DHCPv6 Prefix Delegation, this document assumes that the mobile router uses its egress interface when making DHCPv6 requests.

### 3.2. Deployment Models

This section explains the protocol operation for supporting prefix delegation support in Proxy Mobile IPv6 for the following three deployment models: i) Delegating router co-located with mobile access gateway, ii) Delegating router co-located with local mobility anchor, and iii) Static configuration of delegated prefixes. High-level message call flows between the mobile router, mobile access gateway and the local mobility anchor are presented while explaining the protocol operation.

#### 3.2.1. Delegating Router co-located with Mobile Access Gateway

In this deployment scenario, the delegating router (DR) function, as specified in [RFC3633], is co-located with the mobile access gateway, and a requesting router (RR) function is enabled on the mobile router.

Figure 2 shows the high-level message call flow for this case. The mobile router attaches to the mobile access gateway, which triggers the Proxy Mobile IPv6 signaling between the mobile access gateway and the local mobility anchor, setting up the bi-directional tunnel between them (regular Proxy Mobile IPv6 registration). After that, the DHCPv6 requesting router function running on the mobile router sends a Solicit message requesting a prefix. This message is received by the DHCPv6 delegating router function running on the mobile access gateway. The mobile access gateway then sends a proxy binding update message including a delegated mobile network prefix (DMNP) option carrying the ALL\_ZERO value [RFC5213]. This serves as a request for the local mobility anchor to allocate a set of delegated prefixes, conveyed back in one or more DMNP options in a proxy binding acknowledgment message. The DHCPv6-PD signaling is then completed as described in [RFC3633], finalizing with the delegating router sending a Reply message conveying the delegated prefixes. If the requesting router includes a Rapid Commit option in its Solicit message, it is preferable that the MAG respond directly with a Reply rather than with an Advertise message, as described in [RFC3315], Section 17.2.3.

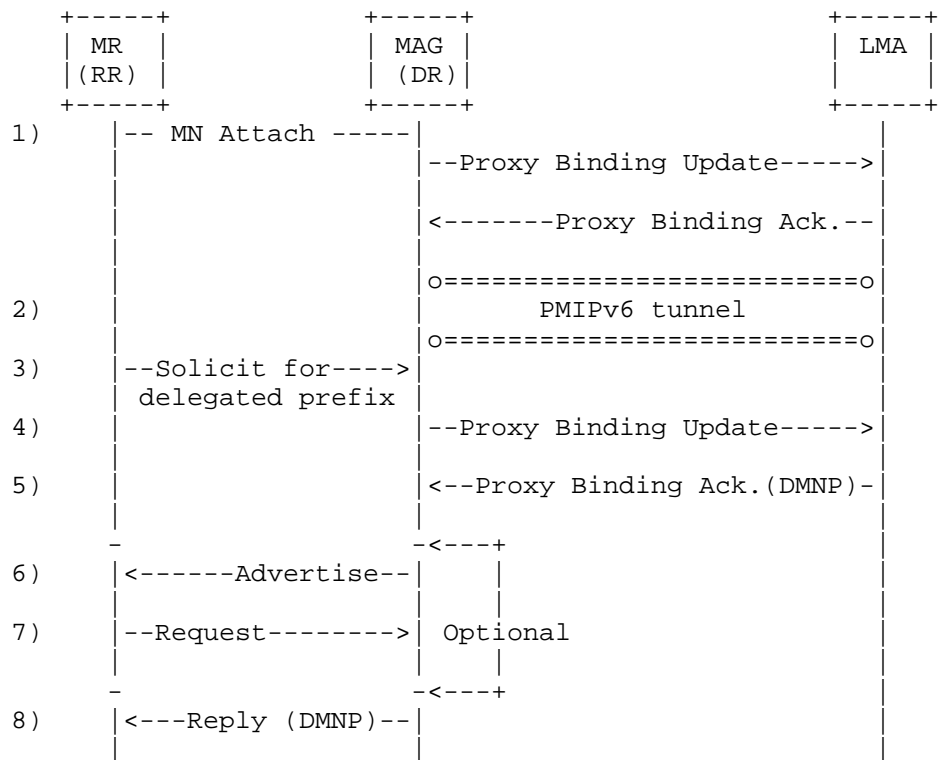


Figure 2: Delegating Router co-located with Mobile Access Gateway

From an operational point of view, this is the simplest deployment option, as it keeps a single protocol interface between the mobile access gateway and the local mobility anchor.

### 3.2.2. Delegating Router co-located with Local Mobility Anchor

In this deployment scenario, the delegating router (DR) function, as specified in [RFC3633], is co-located with the local mobility anchor, the requesting router (RR) function is enabled on the mobile router and a DHCPv6 Relay Agent (DRA) function, is co-located on the mobile access gateway.

Figure 3 shows the high-level message call flow for this case. The mobile router attaches to the mobile access gateway, which triggers the Proxy Mobile IPv6 signaling between the mobile access gateway and the local mobility anchor, setting up the bi-directional tunnel between them (regular Proxy Mobile IPv6 registration). After that, the DHCPv6 requesting router function running on the mobile router requests a prefix by sending a Solicit message. This message is

received by the DHCPv6 relay agent function running on the mobile access gateway, which then completes the DHCPv6 signaling, according to [RFC3315]. The relay agent function SHOULD include the relay agent remote-id option [RFC4649] into Relay-forward messages with appropriate identity information to enable correlation of mobile router identities used over DHCPv6 and PMIPv6.

Once the mobile access gateway gets the set of delegated prefixes from the delegating router function running on the local mobility anchor, the MAG conveys the delegated prefixes in a proxy binding update. This ensures that the local mobility anchor properly routes the traffic addressed to the delegated prefixes via the PMIPv6 tunnel established with the mobile access gateway, and that mobility is provided to these prefixes while the mobile router roams within the PMIPv6 domain. Note that the relay agent function in the mobile access gateway has to queue the Reply message for the duration of the PMIPv6 signaling (steps 10 and 11) before forwarding the Reply message to the requesting router. While this does not change anything from the DHCPv6-PD protocol point of view, implementations will need to account for interactions between the timing of PMIPv6 signaling and the DHCPv6 timeout/retry logic.

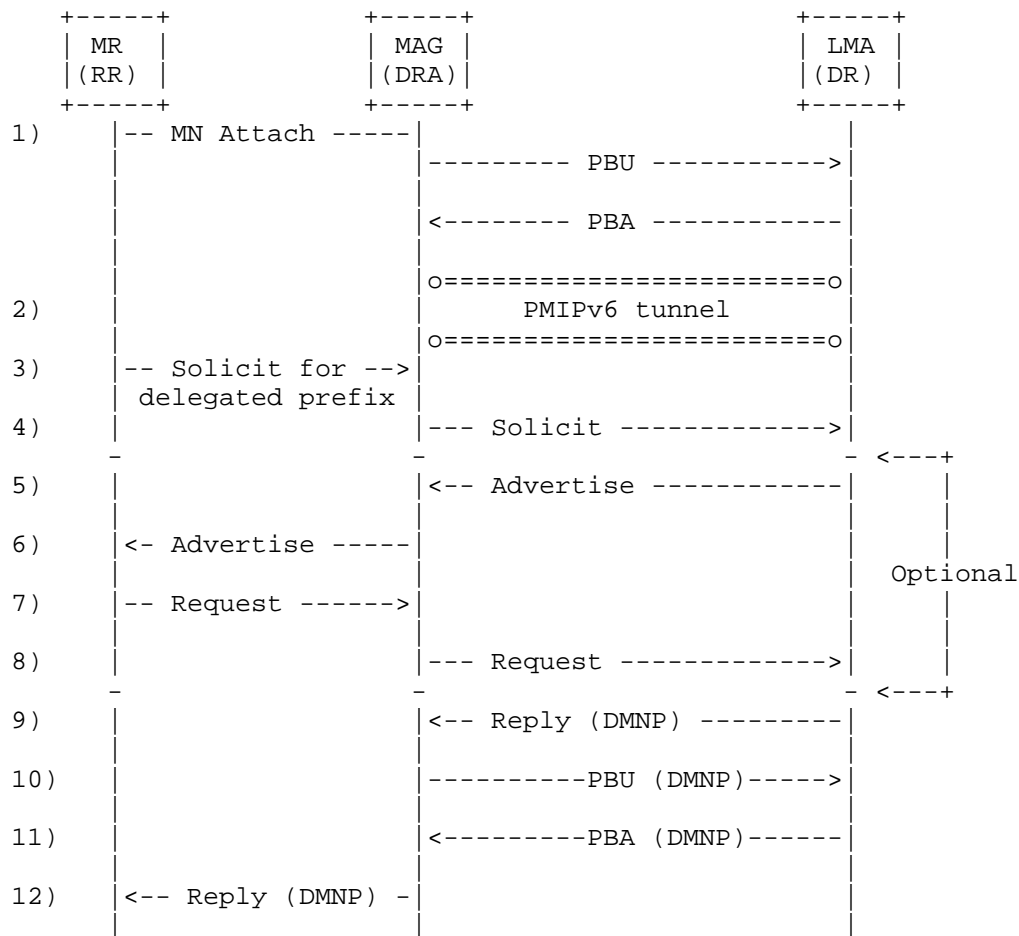


Figure 3: Delegating Router co-located with Local Mobility Anchor

The DR function can also be on the located in other entities of the home network different from the LMA. This deployment model requires some interworking between the DR and the LMA and is out of scope for this specification. Note that this additional interworking would have no impact on the protocol between the LMA and MAG defined in this document.

### 3.2.3. Static Configuration of Delegated Mobile Network Prefixes

In this deployment scenario, the delegated mobile network prefixes of the mobile router are statically configured in the mobile node's policy profile [RFC5213]. The delegated mobile network prefixes are statically configured in the mobile network attached to the mobile

router. The mobile router is the default-router for the mobile networks.

Figure 4 shows a high-level message call flow for this example. The mobile access gateway obtains statically configured mobile network prefixes from the policy profile and registers them with the local mobility anchor using the extensions specified in this document, that is, the use of the delegated mobile network prefix (DMNP) option in the Proxy Mobile IPv6 signaling. There is no explicit trigger from the mobile router for registering, or de-registering those prefixes. As long as there is a mobility session for the mobile router's home address, the local mobility anchor enables mobility support for the mobile network prefixes.

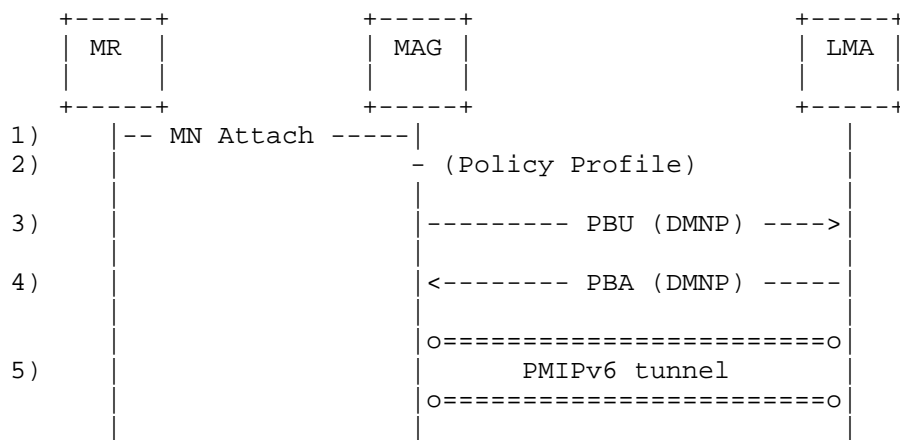


Figure 4: Static Configuration of Delegated Mobile Network Prefixes

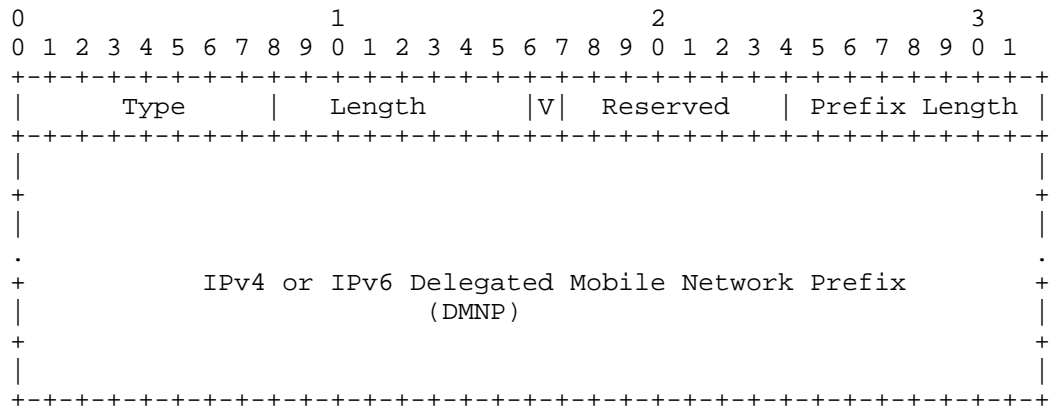
#### 4. Message formats

This section defines extensions to Proxy Mobile IPv6 [RFC5213] protocol messages.

##### 4.1. Delegated Mobile Network Prefix Option

A new mobility header option, Delegated Mobile Network Prefix option is defined for use with Proxy Binding Update and Proxy Binding Acknowledgment messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for exchanging the mobile router's IPv4/IPv6 delegated mobile network prefix. There can be multiple instances of the Delegated Mobile Network Prefix option present in a message.

The Delegated Mobile Network Prefix option has an alignment requirement of  $8n+2$ . Its format is as follows:



#### Type

<IANA-1>: To be assigned by IANA.

#### Length

8-bit unsigned integer indicating the length of the option in octets, excluding the type and length fields.

#### IPv4 Prefix (V)

If the IPv4 Prefix (V) flag is set to a value of (1), then it indicates that the prefix that is included in the DMNP field is an IPv4 prefix. If the IPv4 Prefix (V) flag is set to a value of (0), then it indicates that the prefix that is included in the DMNP field is an IPv6 prefix.

#### Reserved

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

#### Prefix Length

8-bit unsigned integer indicating the prefix length of the prefix contained in the option.

#### Delegated Mobile Network Prefix



Contains a mobile router's 4-byte IPv4 or a 16-byte IPv6 Delegated Mobile Network Prefix.

#### 4.2. Status Codes

This document defines the following new status code values for use in the Proxy Binding Acknowledgement message. These values have been allocated from the same number space as defined in Section 6.1.8 of [RFC6275].

NOT\_AUTHORIZED\_FOR\_DELEGATED\_MNP: <IANA-2>

Not Authorized for delegated mobile network prefix

REQUESTED\_DMNP\_IN\_USE: <IANA-3>

Requested delegated mobile network prefix is in use

#### 5. Operational Details

##### 5.1. MAG Considerations

###### 5.1.1. Extension to Binding Update List Entry Data Structure

In order to support this specification, the conceptual Binding Update List Entry (BULE) data structure [RFC5213] needs to be extended to include a delegated mobile network prefix (DMNP) list. Each entry in the list is used for storing an IPv4/IPv6 mobile network prefix delegated to the mobile router.

###### 5.1.2. Signaling Considerations

During the mobile router's initial attachment procedure, the mobile access gateway obtains the mobile router's policy profile, as per the procedures defined in [RFC5213]. The mobile node's policy profile defined in [RFC5213] is extended to include a parameter which indicates Delegated Prefix support. If the policy profile indicates that the mobile router is authorized for Delegated Prefix support, then the considerations described next apply.

The mobile access gateway MUST include one or more Delegated Mobile Network Prefix (DMNP) options in the Proxy Binding Update message in order to request the local mobility anchor to allocate delegated mobile network prefix(es) for the mobile router.

If the mobile access gateway requests the local mobility anchor to perform the prefix assignment, then:

- o There MUST be exactly one instance of the Delegated Mobile Network Prefix option with ALL\_ZERO value and with the (V) flag set to a value of (0). This serves as a request to the local mobility anchor to allocate a set of delegated IPv6 mobile network prefixes.
- o There MUST be exactly one instance of the Delegated Mobile Network Prefix option with ALL\_ZERO value and with the (V) flag set to a value of (1). This serves as a request to the local mobility anchor to allocate a set of delegated IPv4 mobile network prefixes.
- o If the received Proxy Binding Acknowledgement message has the status field value set to NOT\_AUTHORIZED\_FOR\_DELEGATED\_MNP (Not Authorized for delegated mobile network prefix), the mobile access gateway MUST NOT enable mobility support for any of the prefixes in the mobile network and prefix delegation support has to be disabled.
- o If the received Proxy Binding Acknowledgement message has the status field value set to REQUESTED\_DMNP\_IN\_USE (Requested delegated mobile network prefix is in use), the mobile access gateway MUST NOT enable mobility support for the requested prefixes. The mobile access gateway MAY choose to send Proxy Binding Update message requesting the local mobility anchor to perform the prefix assignment.

If the mobile access gateway provides the local mobility anchor with the prefix(es) that wants to get allocated, then:

- o There MUST be exactly one instance of the Delegated Mobile Network Prefix option with NON\_ZERO prefix value [RFC5213] for each of the mobile network prefixes that the mobile access gateway is requesting the local mobility anchor to allocate. The prefix value in the option is the prefix that is either statically configured for that mobile router in the mobile node's policy profile, or obtained via interactions with the DHCP PD functions. This serves as a request to the local mobility anchor to allocate the requested IPv4/IPv6 prefix.

If the received Proxy Binding Acknowledgement message has the status field value set to 0 (Proxy Binding Update accepted), the mobile access gateway has to apply the following considerations.

- o The delegated mobile network prefix (DMNP) list in the mobile router's Binding Update List entry has to be updated with the allocated prefix(es). However, if the received message was in response to a de-registration request with a lifetime value of

(0), then the delegated mobile network prefix list has to be removed along with the Binding Update List entry.

- o The mobile access gateway has to set up a policy-based route for forwarding the IP packets received from the mobile network (with the source IP address from any of the delegated IPv4/IPv6 mobile network prefixes) through the bidirectional tunnel set up for that mobile router. However, if the received message was in response to a de-registration request with a lifetime value of (0), then the created forwarding state has to be removed.

This specification assumes that all the mobile access gateways of a PMIPv6 Domain support the same prefix delegation mechanism. If there is any difference, it will result in delegated mobile network prefix(es) getting de-registered and the mobile network loosing the prefix(es). This would result in the attached local fixed nodes loosing the assigned IP addresses. The mobile router MAY explicitly deprecate these prefixes. Alternatively the lifetime of the addresses may expire.

#### 5.1.3. DHCP - MAG Interactions

This section describes the interactions between the DHCP and PMIPv6 logical entities running on the mobile access gateway. This section is applicable only for deployments that use DHCPv6-based prefix delegation (i.e., it does not apply if static configuration is used). As described next, these interactions vary slightly depending on the considered deployment model at the mobile access gateway (described in Section 3.2).

The mobile router, acting as a "Requesting Router" as described in [RFC3633], sends a Solicit message including one or more IA\_PD option(s) to the Delegating Router/DHCPv6 Relay Agent collocated on the mobile access gateway. This message provides the needed trigger for the mobile access gateway for requesting the local mobility anchor to enable delegated mobile network prefix support for that mobility session. We next describe the subsequent interactions depending on the deployment model.

##### 5.1.3.1. Delegating Router co-located with Mobile Access Gateway

The mobile access gateway applies the considerations in Section 5.1.2 for requesting the local mobility anchor to enable delegated prefix support. For example, if the mobile router is soliciting an IPv4 prefix, the mobile access gateway includes in the Proxy Binding Update signaling a Delegated Mobile Network Prefix option with ALL\_ZERO value and with the (V) flag set to a value of (1).

The mobile access gateway, upon successfully completing the Proxy Binding Update signaling with the local mobility anchor (following the considerations described in Section 5.1.2), adds the delegated mobile network prefixes to the binding update list. Then, the mobile access gateway provides the obtained prefixes to the DHCPv6 Delegating Router for prefix assignment. The way in which these prefixes are passed to the DHCPv6 delegating router function is beyond the scope of this document.

- o In case the Proxy Binding Update signaling with the local mobility anchor is not completed successfully, for example because the local mobility anchor is not authorized for delegated mobile network prefix or the requested prefix is in use, the DHCPv6 Delegating Router will send a Reply message to the Requesting Router with no IA\_PREFIX suboptions and with a Status Code option as described in [RFC3633], section 11.2.

The standard DHCPv6 considerations will be applied with respect to the interactions between the Delegating Router and the Requesting Router. The Requesting Router is provided with the delegated prefix(es), which can then be then advertised in the mobile network, and therefore used by the locally fixed nodes to auto configure IP addresses allowing to gain access to the Internet.

Any time, the Requesting Router releases the delegated prefixes, the Delegating Router removes the assigned prefixes. To do so, the mobile access gateway will send an Updated Proxy Binding Update following the considerations described in Section 5.1.2 for de-registering those prefixes. The way in which the DHCPv6 Delegating Router triggers the mobile access gateway in order to de-register the prefixes is beyond the scope of this document.

In case the mobile router performs a handover and attaches to a different mobile access gateway, the following cases are possible:

- o The new mobile access gateway does not support the delegation of mobile network prefixes described in this specification. In this case, forwarding of the previously delegated mobile network prefixes is no longer performed.
- o The new mobile access gateway supports the delegation of mobile network prefixes described in this specification. There are two possible cases upon the reception of the SOLICIT message by the Delegating Router. If the MAG already knows the delegated mobile network prefixes, it conveys them in a DMNP option included in the Proxy Binding Update sent to the local mobility anchor, which then authorizes them based on: a) the content of the associated binding cache entry (if exists), b) the user profile (if the allocation is

static), or, c) checking that the delegated mobile network prefixes are not already allocated. On the other hand, if the mobile access gateway is not aware of the delegated mobile network prefixes, it will include 0.0.0.0 / ::0 in a DMNP option included in the Proxy Binding Update sent to the LMA, which will provide the right prefixes back in the Proxy Binding Acknowledgement based on a) the content of the associated binding cache entry (if exists), b) the profile (if static allocation is used), or c) dynamic assignment.

#### 5.1.3.2. Delegating Router co-located with Local Mobility Anchor

A DHCPv6 Relay Agent function running on the mobile access gateway will forward the DHCP messages to the local mobility anchor which has the co-located Delegating Router function. The Requesting Router and the Delegating Router complete the DHCP messages related to prefix delegation.

During the DHCPv6 exchange, the standard DHCPv6 considerations apply with respect to the interactions between the Delegating Router, DHCPv6 Relay Agent and the Requesting Router.

The mobile access gateway learns from the co-located DHCPv6 Relay Agent the prefixes allocated by the Delegating Router. The way in which the mobile access gateway learns obtains this information from the DHCPv6 Relay Agent function is beyond the scope of this document.

The mobile access gateway will apply the considerations in Section 5.1.2 for requesting the local mobility anchor to enable delegated prefix support. The mobile access gateway will include exactly one instance of the Delegated Mobile Network Prefix option with NON\_ZERO prefix value for each of the mobile network prefixes that the mobile access gateway is requesting the local mobility anchor to allocate. The prefix value(s) in the option will be the prefix(es) obtained via DHCP prefix delegation.

The mobile access gateway, upon successfully completing the Proxy Binding Update signaling with the local mobility anchor, will provide the obtained prefixes to the DHCPv6 Relay Agent for prefix assignment. The Delegating Router is provided with the delegated prefix(es) completing the standard DHCPv6 signaling. These prefixes can then be then advertised in the mobile network, and therefore used by the locally fixed nodes to auto configure IP addresses allowing to gain access to the Internet.

- o In case the Proxy Binding Update signaling with the local mobility anchor is not completed successfully, for example because the local mobility anchor is not authorized for delegated mobile

network prefix, the requested prefix is in use, or the delegated prefix(es) do not match the ones allocated by DHCP prefix delegation, the DHCPv6 Relay Agent MAY send a Reply message to the Requesting Router with no IA\_PREFIX suboptions and with a Status Code option as described in [RFC3633], section 11.2.

In case the mobile router performs a handover and attaches to a different mobile access gateway, the following cases are possible:

- o The new mobile access gateway does not support the delegation of mobile network prefixes described in this specification. In this case, forwarding of the previously delegated mobile network prefixes is no longer performed.
- o The new mobile access gateway supports the delegation of mobile network prefixes described in this specification. There are two possible cases upon the reception of the SOLICIT message by the DHCPv6 Relay Agent. If the MAG already knows the delegated mobile network prefixes, it conveys them in a DMNP option included in the Proxy Binding Update sent to the local mobility anchor, which then authorizes them based on: a) the content of the associated binding cache entry (if exists), b) the user profile (if the allocation is static), or, c) checking that the delegated mobile network prefixes are not already allocated. On the other hand, if the mobile access gateway is not aware of the delegated mobile network prefixes, it will include 0.0.0.0 / ::0 in a DMNP option included in the Proxy Binding Update sent to the LMA, which will provide the right prefixes back in the Proxy Binding Acknowledgement based on a) the content of the associated binding cache entry (if exists), b) the profile (if static allocation is used), or c) dynamic assignment.

#### 5.1.4. Packet Forwarding

On receiving an IP packet from a mobile router, the mobile access gateway before tunneling the packet to the local mobility anchor MUST ensure that there is an established binding for the mobile router and the source IP address of the packet is a prefix delegated to that mobile router. If the source address of the received IP packet is not part of the delegated mobile network prefix, then the mobile access gateway MUST NOT tunnel the packet to the local mobility anchor.

On receiving an IP packet from the bi-directional tunnel established with the local mobility anchor, the mobile access gateway MUST first decapsulate the packet (removing the outer header) and then use the destination address of the (inner) packet to forward it on the interface through which the mobile router is reachable.

The above forwarding considerations are not applicable to the IP traffic sent/received to/from the mobile router's home address (IPv4 HOA/HNP). For the mobile router's home address traffic, forwarding considerations from [RFC5213] and [RFC5844] continue to apply.

## 5.2. LMA Considerations

### 5.2.1. Extensions to Binding Cache Entry Data Structure

In order to support this specification, the conceptual Binding Cache Entry (BCE) data structure [RFC5213] needs to be extended to include the delegated mobile network prefix (DMNP) list. Each entry in the list represents a delegated mobile network prefix.

### 5.2.2. Signaling Considerations

If the Proxy Binding Update message does not include any Delegated Mobile Network Prefix option(s) (Section 4.1), then the local mobility anchor MUST NOT enable Delegated Prefix support for the mobility session, and the Proxy Binding Acknowledgment message that is sent in response MUST NOT contain any Delegated Mobile Network Prefix option(s).

If the Proxy Binding Update message includes one or more Delegated Mobile Network Prefix options, but the local mobility anchor is not configured with Delegated Prefix support, then the local mobility anchor will ignore the option(s) and process the rest of the option as specified in [RFC5213]. This would have no effect on the operation of the rest of the protocol. The Proxy Binding Acknowledgment message that is sent in response will not include any Delegated Mobile Network Prefix option(s).

If the Proxy Binding Update message has the Delegated Mobile Network Prefix option(s) and if the local mobility anchor is configured for Delegated Prefix support, then the local mobility anchor MUST enable Delegated Mobile Network Prefix option for that mobility session. The Proxy Binding Acknowledgment message that is sent in response MUST include the Delegated Mobile Network Prefix option(s). The following considerations apply.

- o If there is at least one instance of the Delegated Mobile Network Prefix option with a ALL\_ZERO [RFC5213] prefix value, then this serves as a request for the local mobility anchor to perform the assignment of one or more delegated mobile network prefixes.
- \* A Delegated Mobile Network option with ALL\_ZERO value and with the (V) flag set to a value of (0), is a request for the local mobility anchor to allocate one or more IPv6 prefixes.

- \* A Delegated Mobile Network option with ALL\_ZERO value and with the (V) flag set to a value of (1), is a request for the local mobility anchor to allocate one or more IPv4 prefixes.
- \* Inclusion of multiple instances of Delegated Mobile Network options with ALL\_ZERO value, one with the (V) flag set to a value of (1), and another instance with the (V) flag set to a value of (0) is a request to allocate both IPv4 and IPv6 prefixes.
- o If there are no instances of the Delegated Mobile Network Prefix option present in the request with ALL\_ZERO value, but has a specific prefix value, then this serves as a request for the local mobility anchor to perform the allocation of the requested prefix(es).
- \* If any one of the requested prefixes are assigned to some other mobility node, or not from an authorized pool that the local mobility can allocate for that mobility session, then the Proxy Binding Update MUST be rejected by sending a Proxy Binding Acknowledgement message with Status field set to REQUESTED\_DMNP\_IN\_USE (Requested delegated mobile network prefix is in use).

Upon accepting the Proxy Binding Update, the local mobility anchor MUST send a Proxy Binding Acknowledgement message with the Status field set to 0 (Proxy Binding Update accepted).

- o The message MUST include one instance of the Delegated Mobile Network Prefix option for each of the allocated IPv4/IPv6 delegated mobile network prefixes.
- o The delegated mobile network prefix (DMNP) list in the mobile router's Binding Cache entry has to be updated with the allocated prefix(es). However, if the request is a de-registration request with a lifetime value of (0), the delegated mobile network prefix list has to be removed along with the Binding Cache entry.
- o A route (or a platform-specific equivalent function that sets up the forwarding) for each of the allocated prefixes over the tunnel has to be added. However, if the request is a de-registration request, with a lifetime value of (0), all the IPv4/IPv6 delegated prefix routes created for that session have to be removed.



### 5.2.3. Packet Forwarding

The local mobility anchor MUST advertise a connected route into the routing infrastructure for the IP prefixes delegated to all of the mobile routers that it is serving. This step essentially enables the local mobility anchor to be a routing anchor for those IP prefixes and be able to intercept IP packets sent to those mobile networks.

On receiving a packet from a correspondent node with the destination address matching any of the mobile router's delegated mobile network prefixes, the local mobility anchor MUST forward the packet through the bi-directional tunnel set up with the mobile access gateway where the mobile router is attached.

On receiving an IP packet from the bi-directional tunnel established with the mobile access gateway, the local mobility anchor MUST first decapsulate the packet (removing the outer header) and then use the destination address of the (inner) packet for forwarding decision. The local mobility anchor MUST ensure that there is an established binding for the mobile router and the source IP address of the packet is a prefix delegated to a mobile router reachable over that bi-directional tunnel.

The above forwarding considerations are not applicable to the IP traffic sent/received to/from the mobile router's home address (IPv4 HOA/HNP). For the mobile router's home address traffic, forwarding considerations from [RFC5213] and [RFC5844] continue to apply.

### 5.3. Security Policy Database (SPD) Example Entries

The use of DHCPv6, as described in this document, requires message integrity protection and source authentication. The IPsec security mechanism used by Proxy Mobile IPv6 [RFC5213] for securing the signaling messages between the mobile access gateway and the local mobility anchor can be used for securing the DHCP signaling between the mobile access gateway and the local mobility anchor.

The Security Policy Database (SPD) and Security Association Database (SAD) entries necessary to protect the DHCP signaling is specified below. The format of these entries is based on [RFC4877] conventions. The SPD and SAD entries are only example configurations. A particular implementation of mobile access gateway and local mobility anchor implementation can configure different SPD and SAD entries as long as they provide the required security for protecting DHCP signaling messages.

For the examples described in this document, a mobile access gateway with address "mag\_address\_1", and a local mobility anchor with

address "lma\_address\_1" are assumed.

mobile access gateway SPD-S:

- IF local\_address = mag\_address\_1 &  
remote\_address = lma\_address\_1 & proto = UDP &  
local\_port = any & remote\_port = DHCP  
Then use SA1 (OUT) and SA2 (IN)

mobile access gateway SAD:

- SA1(OUT, spi\_a, lma\_address\_1, ESP, TRANSPORT):  
local\_address = mag\_address\_1 &  
remote\_address = lma\_address\_1 &  
proto = UDP & remote\_port = DHCP
- SA2(IN, spi\_b, mag\_address\_1, ESP, TRANSPORT):  
local\_address = lma\_address\_1 &  
remote\_address = mag\_address\_1 &  
proto = UDP & local\_port = DHCP

local mobility anchor SPD-S:

- IF local\_address = lma\_address\_1 &  
remote\_address = mag\_address\_1 & proto = UDP &  
local\_port = DHCP & remote\_port = any  
Then use SA2 (OUT) and SA1 (IN)

local mobility anchor SAD:

- SA2(OUT, spi\_b, mag\_address\_1, ESP, TRANSPORT):  
local\_address = lma\_address\_1 &  
remote\_address = mag\_address\_1 &  
proto = UDP & local\_port = DHCP
- SA1(IN, spi\_a, lma\_address\_1, ESP, TRANSPORT):  
local\_address = mag\_address\_1 &  
remote\_address = lma\_address\_1 &  
proto = UDP & remote\_port = DHCP

## 6. Security Considerations

The Delegated Mobile Network Prefix Option defined in this specification is for use in Proxy Binding Update and Proxy Binding Acknowledgement messages. This option is carried like any other mobility header option as specified in [RFC5213]. Therefore, it inherits from [RFC5213] its security guidelines and does not require any additional security considerations.

The use of DHCPv6 in this specification is as defined in DHCPv6 base specification [RFC3315] and DHCPv6 Prefix Delegation specifications [RFC3633]. The security considerations specified in those specifications apply to this document.

If IPsec is used, the IPsec security association that is used for protecting the Proxy Binding Update and Proxy Binding Acknowledgement, also needs to be used for protecting the DHCPv6 signaling between the mobile access gateway and the local mobility anchor. Considerations specified in Section 5.3 identify the extensions to security policy entries [RFC4301]

## 7. IANA Considerations

This document requires the following IANA actions.

- o Action-1: This specification defines a new Mobility Header option, Delegated Mobile Network Prefix option. This mobility option is described in Section 4.1. The type value <IANA-1> for this message needs to be allocated from the Mobility Options registry at <http://www.iana.org/assignments/mobility-parameters>. RFC Editor: Please replace <IANA-1> in Section 4.1 with the assigned value, and update this section accordingly.
- o Action-2: This document also defines two new status code values for use in the Proxy Binding Acknowledgement message, as described in Section 4.2. These status codes are, NOT\_AUTHORIZED\_FOR\_DELEGATED\_MNP (Not Authorized for delegated mobile network prefix) with a status code value of <IANA-2>, and REQUESTED\_DMNP\_IN\_USE (Requested delegated mobile network prefix is in use) with a status code value of <IANA-3>. These values have to be assigned from the same number space as allocated for other status codes [RFC6275] and update this section accordingly.

## 8. Acknowledgments

The authors would like to acknowledge Ryuji Wakikawa, Alexandru Petrescu, Behcet Sarikaya, Seil Jeon, Basavaraj Patil, Brian Haberman and Michal Hoefft for all the discussions and reviews of this draft.

The work of Carlos J. Bernardos has also been partially supported by the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project) and by the Ministry of Science and Innovation of Spain under the QUARTET project (TIN2009-13992-C02-01).

## 9. References

### 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- [RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, August 2006.
- [RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6276] Droms, R., Thubert, P., Dupont, F., Haddad, W., and C. Bernardos, "DHCPv6 Prefix Delegation for Network Mobility (NEMO)", RFC 6276, July 2011.
- [RFC6603] Korhonen, J., Savolainen, T., Krishnan, S., and O. Troan, "Prefix Exclude Option for DHCPv6-based Prefix Delegation", RFC 6603, May 2012.

### 9.2. Informative References

- [RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, July 2007.
- [RFC6656] Johnson, R., Kinnear, K., and M. Stapp, "Description of Cisco Systems' Subnet Allocation Option for DHCPv4",

RFC 6656, July 2012.

Authors' Addresses

Xingyue Zhou  
ZTE Corporation  
No.50 Software Avenue, Yuhuatai District  
Nanjing  
China

Phone: +86-25-8801-4634  
Email: zhou.xingyue@zte.com.cn

Jouni Korhonen  
Broadcom  
Porkkalankatu 24  
Helsinki FIN-00180  
Finland

Email: jouni.nospam@gmail.com

Carl Williams  
Consultant  
San Jose, CA  
USA

Email: carlw@mcsr-labs.org

Sri Gundavelli  
Cisco  
170 West Tasman Drive  
San Jose, CA 95134  
USA

Email: sgundave@cisco.com

Carlos J. Bernardos  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain

Phone: +34 91624 6236  
Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)  
URI: <http://www.it.uc3m.es/cjbc/>



NETEXT Working Group  
Internet-Draft  
Updates: 5213 (if approved)  
Intended status: Standards Track  
Expires: September 19, 2016

CJ. Bernardos, Ed.  
UC3M  
March 18, 2016

Proxy Mobile IPv6 Extensions to Support Flow Mobility  
draft-ietf-netext-pmipv6-flowmob-18

Abstract

Proxy Mobile IPv6 allows a mobile node to connect to the same Proxy Mobile IPv6 domain through different interfaces. This document describes extensions to the Proxy Mobile IPv6 protocol that are required to support network based flow mobility over multiple physical interfaces.

This document updates RFC 5213. The extensions described in this document consist of the operations performed by the local mobility anchor and the mobile access gateway to manage the prefixes assigned to the different interfaces of the mobile node, as well as how the forwarding policies are handled by the network to ensure consistent flow mobility management.

Requirements Language

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 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on September 19, 2016.



## Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
3. Overview of the PMIPv6 flow mobility extensions . . . . .	4
3.1. Use case scenarios . . . . .	4
3.2. Basic Operation . . . . .	5
3.2.1. MN sharing a common set of prefixes on all MAGs . . . . .	5
3.2.2. MN with different sets of prefixes on each MAG . . . . .	9
3.3. Use of PBU/PBA signaling . . . . .	11
3.4. Use of flow-level information . . . . .	12
4. Message Formats . . . . .	12
4.1. Home Network Prefix . . . . .	12
4.2. Flow Mobility Initiate (FMI) . . . . .	13
4.3. Flow Mobility Acknowledgement (FMA) . . . . .	14
5. Conceptual Data Structures . . . . .	14
5.1. Multiple Proxy Care-of Address Registration . . . . .	14
5.2. Flow Mobility Cache . . . . .	15
6. Mobile Node considerations . . . . .	16
7. IANA Considerations . . . . .	16
8. Security Considerations . . . . .	17
9. Authors . . . . .	17
10. Acknowledgments . . . . .	18
11. References . . . . .	18
11.1. Normative References . . . . .	18
11.2. Informative References . . . . .	19
Author's Address . . . . .	19

## 1. Introduction

Proxy Mobile IPv6 (PMIPv6), specified in [RFC5213], provides network based mobility management to hosts connecting to a PMIPv6 domain. PMIPv6 introduces two new functional entities, the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The MAG is the entity detecting the Mobile Node's (MN) attachment and providing IP connectivity. The LMA is the entity assigning one or more Home Network Prefixes (HNP) to the MN and is the topological anchor for all traffic belonging to the MN.

PMIPv6 allows a mobile node to connect to the same PMIPv6 domain through different interfaces. This document specifies protocol extensions to Proxy Mobile IPv6 between the local mobility anchor and mobile access gateways to enable "flow mobility" and hence distribute specific traffic flows on different physical interfaces. It is assumed that the mobile node IP layer interface can simultaneously and/or sequentially attach to multiple MAGs, possibly over multiple media. One form to achieve this multiple attachment is described in [I-D.ietf-netext-logical-interface-support], which allows the mobile node supporting traffic flows on different physical interfaces regardless of the assigned prefixes on those physical interfaces. Another alternative is to configure the IP stack of the mobile node to behave according to the weak host model [RFC1122].

In particular, this document specifies how to enable "flow mobility" in the PMIPv6 network (i.e., local mobility anchors and mobile access gateways). In order to do so, two main operations are required: i) proper prefix management by the PMIPv6 network, and, ii) consistent flow forwarding policies. This memo analyzes different potential use case scenarios, involving different prefix assignment requirements, and therefore different PMIPv6 network extensions to enable "flow mobility".

## 2. Terminology

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 [RFC2119].

The following terms used in this document are defined in the Proxy Mobile IPv6 [RFC5213]:

Local Mobility Agent (LMA).

Mobile Access Gateway (MAG).

Proxy Mobile IPv6 Domain (PMIPv6-Domain).

LMA Address (LMAA).

Proxy Care-of Address (Proxy-CoA).

Home Network Prefix (HNP).

The following terms used in this document are defined in the Multiple Care-of Addresses Registration [RFC5648] and Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support [RFC6089]:

Binding Identification Number (BID).

Flow Identifier (FID).

Traffic Selector (TS).

The following terms are defined and used in this document:

FMI (Flow Mobility Initiate). Message sent by the LMA to the MAG conveying the information required to enable flow mobility in a PMIPv6-Domain.

FMA (Flow Mobility Acknowledgement). Message sent by the MAG in reply to an FMI message.

FMC (Flow Mobility Cache). Conceptual data structure to support the flow mobility management operations described in this document.

### 3. Overview of the PMIPv6 flow mobility extensions

#### 3.1. Use case scenarios

In contrast to a typical handover where connectivity to a physical medium is relinquished and then re-established, flow mobility assumes a mobile node can have simultaneous access to more than one network. In this specification, it is assumed that the local mobility anchor is aware of the mobile node's capabilities to have simultaneous access to both access networks and it can handle the same or a different set of prefixes on each access. How this is done is outside the scope of this specification.

There are different flow mobility scenarios. In some of them the mobile node might share a common set of prefixes among all its physical interfaces, whereas in others the mobile node might have a different subset of prefixes configured on each of the physical interfaces. The different scenarios are the following:

1. At the time of a new network attachment, the MN obtains the same prefix or the same set of prefixes as already assigned to an existing session. This is not the default behavior with basic PMIPv6 [RFC5213], and the LMA needs to be able to provide the same assignment even for the simultaneous attachment (as opposed to the handover scenario only).
2. At the time of a new network attachment, the MN obtains a new prefix or a new set of prefixes for the new session. This is the default behavior with basic PMIPv6 [RFC5213].

A combination of the two above-mentioned scenarios is also possible. At the time of a new network attachment, the MN obtains a combination of prefix(es) in use and new prefix(es). This is a hybrid of the two scenarios described before. The local policy determines whether the new prefix is exclusive to the new attachment or it can be assigned to an existing attachment as well.

The operational description of how to enable flow mobility in each of these scenarios is provided in Section 3.2.1 and Section 3.2.2.

The extensions described in this document support all the aforementioned scenarios.

### 3.2. Basic Operation

This section describes how the PMIPv6 extensions described in this document enable flow mobility support.

Both the mobile node and the local mobility anchor MUST have local policies in place to ensure that packets are forwarded coherently for unidirectional and bidirectional communications. The details about how this consistency is ensured are out of the scope of this document. Either the MN or the LMA can initiate IP flow mobility. If the MN makes the flow mobility decision, then the LMA follows that decision and updates its forwarding state accordingly. The network can also trigger mobility on the MN side via out-of-band mechanisms (e.g., 3GPP/ANDSF sends updated routing policies to the MN). In a given scenario and mobile node, the decision on IP flow mobility MUST be taken either by the MN or the LMA, but MUST NOT be taken by both.

#### 3.2.1. MN sharing a common set of prefixes on all MAGs

This scenario corresponds to the first use case scenario described in Section 3.1. Extensions to basic PMIPv6 [RFC5213] signaling at the time of a new attachment are needed to ensure that the same prefix (or set of prefixes) is assigned to all the interfaces of the same mobile node that are simultaneously attached. Subsequently, no

further signaling is necessary between the local mobility anchor and the mobile access gateway and flows are forwarded according to policy rules on the local mobility anchor and the mobile node.

If the local mobility anchor assigns a common prefix (or set of prefixes) to the different physical interfaces attached to the domain, then every MAG already has all the routing knowledge required to forward uplink or downlink packets after the PBU/PBA registration for each MAG, and the local mobility anchor does not need to send any kind of signaling in order to move flows across the different physical interfaces (because moving flows is a local decision of the LMA). Optionally, signaling MAY be exchanged in case the MAG needs to know about flow level information (e.g., to link flows with proper QoS paths and/or inform the mobile node) [RFC7222].

The local mobility anchor needs to know when to assign the same set of prefixes to all the different physical interfaces of the mobile node. This can be achieved by different means, such as policy configuration, default policies, etc. In this document a new Handoff Indicator (HI) value ("Attachment over a new interface sharing prefixes", value {IANA-0}) is defined, to allow the mobile access gateway to indicate to the local mobility anchor that the same set of prefixes MUST be assigned to the mobile node. The considerations of Section 5.4.1 of [RFC5213] are updated by this specification as follows:

- o If there is at least one Home Network Prefix option present in the request with a NON\_ZERO prefix value, there exists a Binding Cache entry (with all home network prefixes in the Binding Cache entry matching the prefix values of all Home Network Prefix options of the received Proxy Binding Update message), and the entry matches the mobile node identifier in the Mobile Node Identifier option of the received Proxy Binding Update message, and the value of the Handoff Indicator of the received Proxy Binding Update is equal to "Attachment over a new interface sharing prefixes".
  1. If there is an MN-LL-Identifier Option present in the request and the Binding Cache entry matches the Access Technology Type (ATT), and MN-LL-Identifier, the request MUST be considered as a request for updating that Binding Cache entry.
  2. If there is an MN-LL-Identifier Option present in the request and the Binding Cache entry does not match the Access Technology Type (ATT), and MN-LL-Identifier, the request MUST be considered as a request for creating a new mobility session sharing the same set of home network prefixes assigned to the existing Binding Cache entry found.

3. If there is not an MN-LL-Identifier Option present in the request, the request MUST be considered as a request for creating a new mobility session sharing the same set of home network prefixes assigned to the existing Binding Cache entry found.

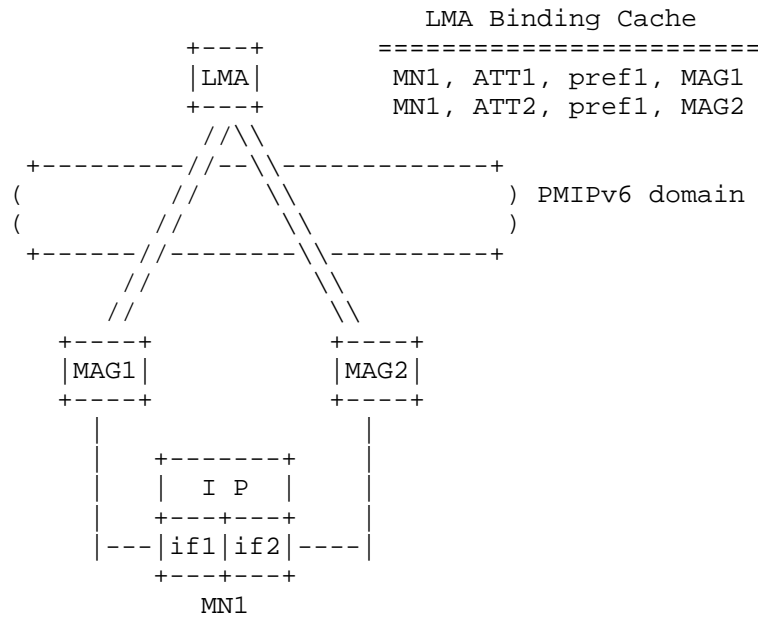


Figure 1: Shared prefix across physical interfaces scenario

Next, an example of how flow mobility works in this case is shown. In Figure 1, a mobile node (MN1) has two different physical interfaces (if1 of access technology type ATT1, and if2 of access technology type ATT2). Each physical interface is attached to a different mobile access gateway, both of them controlled by the same local mobility anchor. Both physical interfaces are assigned the same prefix (pref1) upon attachment to the MAGs. If the IP layer at the mobile node shows one single logical interface (e.g., as described in [I-D.ietf-netext-logical-interface-support]), then the mobile node has one single IPv6 address configured at the IP layer: pref1::mn1. Otherwise, per interface IPv6 addresses (e.g., pref1::if1 and pref1::if2) would be configured; each address MUST be valid on every interface. We assume the first case in the following example (and in the rest of this document). Initially, flow X goes through MAG1 and flow Y through MAG2. At a certain point, flow Y can be moved to also go through MAG1. Figure 2 shows the scenario in which no flow-level information needs to be exchanged, so there is no

signaling between the local mobility anchor and the mobile access gateways.

Note that if different IPv6 addresses are configured at the IP layer, IP session continuity is still possible (for each of the configured IP addresses). This is achieved by the network delivering packets destined to a particular IP address of the mobile node to the right MN's physical interface where the flow is selected to be moved, and the MN also selecting the same interface when sending traffic back up link.

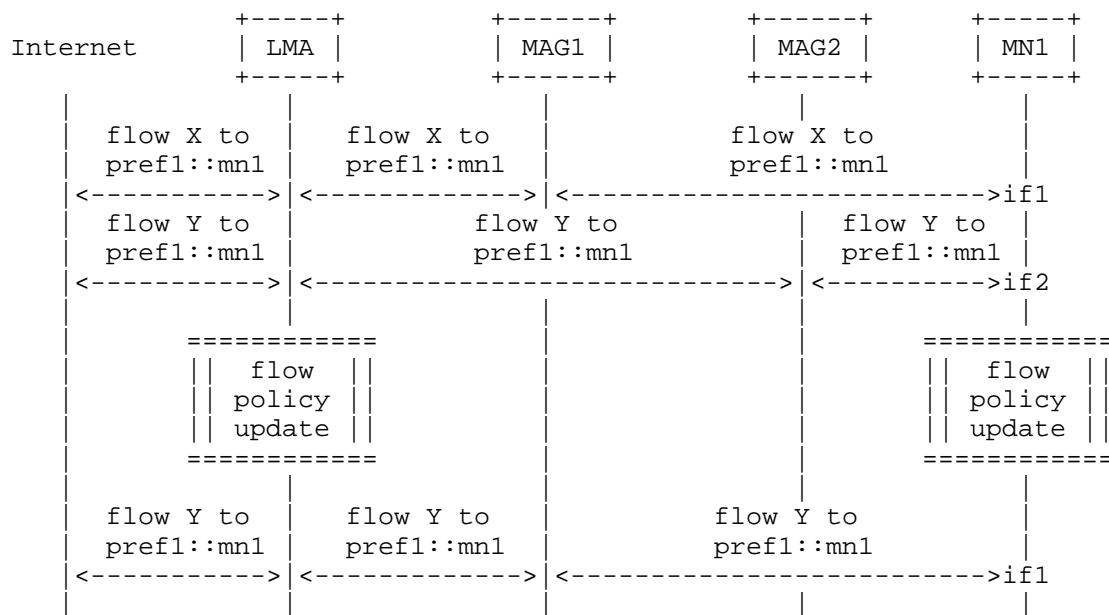


Figure 2: Flow mobility message sequence with common set of prefixes

Figure 3 shows the state of the different network entities after moving flow Y in the previous example. This document re-uses some of the terminology and mechanisms of the flow bindings and multiple care-of address registration specifications. Note that, in this case the BIDs shown in the figure are assigned locally by the LMA, since there is no signaling required in this scenario. In any case, alternative implementations of flow routing at the LMA MAY be used, as it does not impact on the operation of the solution in this case.

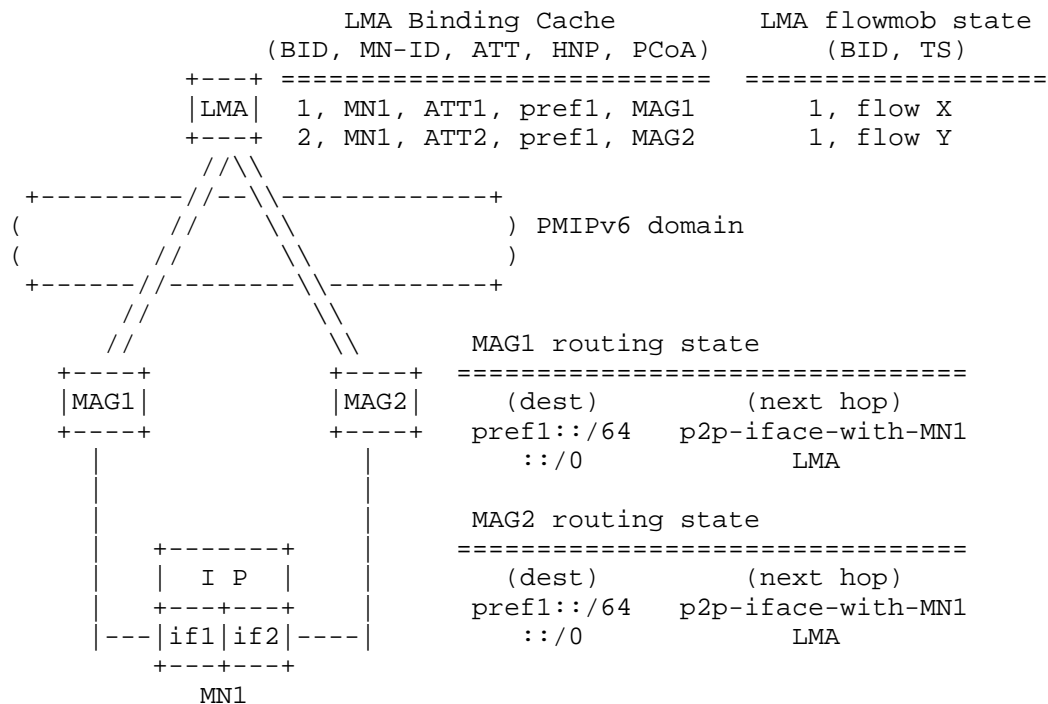


Figure 3: Data structures with common set of prefixes

### 3.2.2. MN with different sets of prefixes on each MAG

A different flow mobility scenario happens when the local mobility anchor assigns different sets of prefixes to physical interfaces of the same mobile node. This covers the second case, or a combination of scenarios, described in Section 3.1. In this case, additional signaling is required between the local mobility anchor and the mobile access gateway to enable relocating flows between the different attachments, so the MAGs are aware of the prefixes for which the MN is going to receive traffic, and local routing entries are configured accordingly.

In this case, signaling is required when a flow is to be moved from its original interface to a new one. Since the local mobility anchor cannot send a PBA message which has not been triggered in response to a received PBU message, the solution defined in this specification makes use of two mobility messages: Flow Mobility Indication and Flow Mobility Acknowledgement, which actually use the format of the Update Notifications for Proxy Mobile IPv6 defined in [RFC7077]. The trigger for the flow movement can be on the mobile node (e.g., by using layer-2 signaling with the MAG) or on the network (e.g., based



on congestion and measurements) which then notifies the MN for the final IP flow mobility decision (as stated in section 3.1). Policy management functions (e.g., 3GPP/ANDSF) can be used for that purpose, however, how the network notifies the MN is out of the scope of this document.

If the flow is being moved from its default path (which is determined by the destination prefix) to a different one, the local mobility anchor constructs a Flow Mobility Indication (FMI) message. This message includes a Home Network Prefix option for each of the prefixes that are requested to be provided with flow mobility support on the new MAG (note that these prefixes are not anchored by the target MAG, and therefore the MAG MUST NOT advertise them on the MAG-MN link), with the off-link bit (L) set to one. This message MUST be sent to the new target mobile access gateway, i.e. the one selected to be used in the forwarding of the flow. The MAG replies with a Flow Mobility Acknowledgement (FMA). The message sequence is shown in Figure 4.

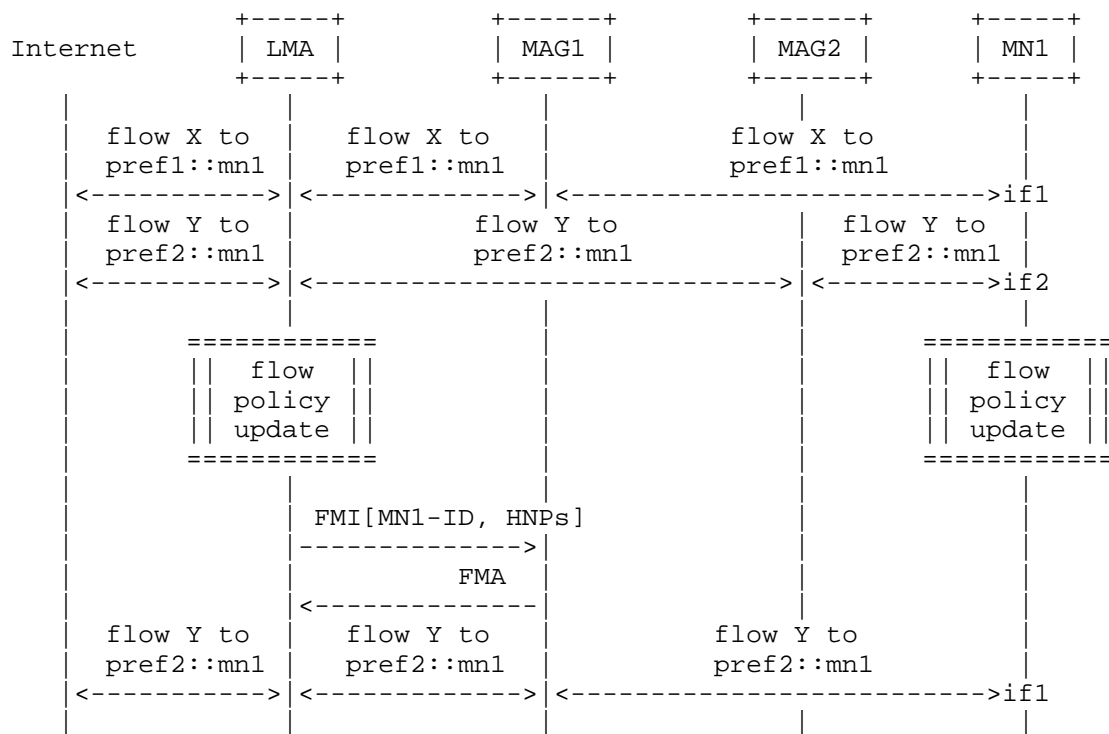


Figure 4: Flow mobility message sequence when the LMA assigns different sets of prefixes per physical interface

The state in the network after moving a flow, for the case the LMA assigns a different set of prefixes is shown in Figure 5.

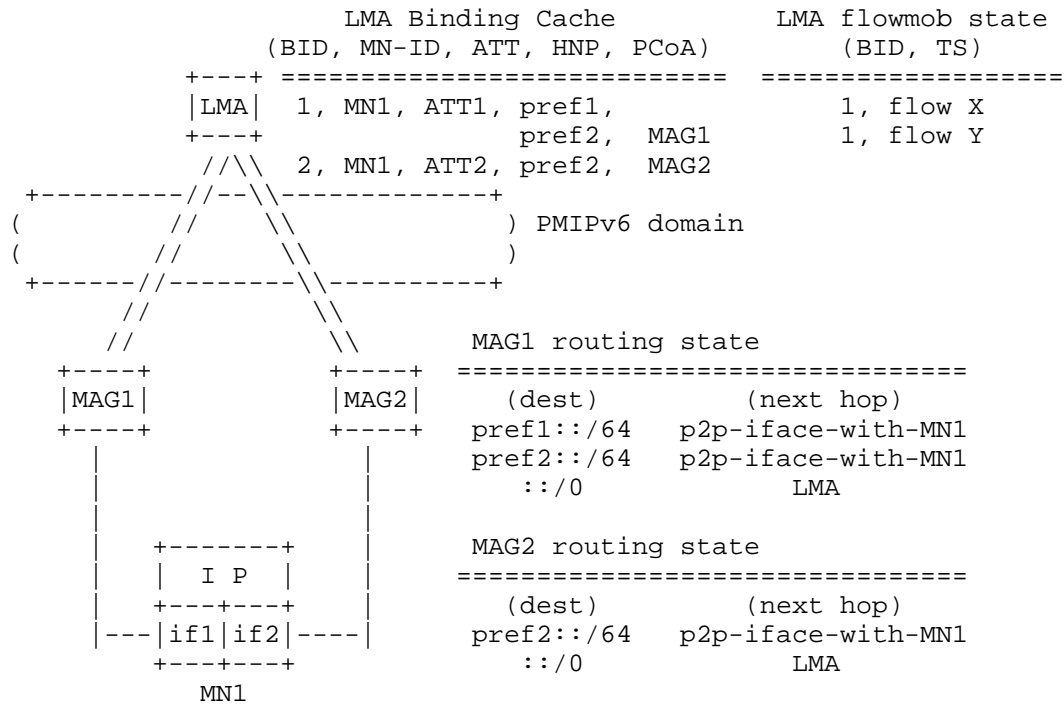


Figure 5: Data structures when the LMA assigns a different set of prefixes

### 3.3. Use of PBU/PBA signaling

This specification introduces the FMI/FMA signaling so the LMA can exchange with the MAG information required to enable flow mobility without waiting for receiving a PBU. There are however scenarios in which the trigger for flow mobility might be related to a new MN's interface attachment. In this case, the PBA sent in response to the PBU received from the new MAG can convey the same signaling that the FMI does. In this case the LMA MUST include in the PBA a Home Network Prefix option for each of the prefixes that are requested to be provided with flow mobility support on the new MAG with the off-link bit (L) set to one.

### 3.4. Use of flow-level information

This specification does not mandate flow-level information to be exchanged between the LMA and the MAG to provide flow mobility support. It only requires the LMA to keep flow-level state (Section 5.2). However, there are scenarios in which the MAG might need to know which flow(s) is/are coming within a prefix that has been moved, to link it/them to proper QoS path(s) and optionally inform the MN about it. This section describes the extensions used to include flow-level information in the signaling defined between the LMA and the MAG.

This specification re-uses some of the mobility extensions and message formats defined in [RFC5648] and [RFC6089], namely the Flow Identification Mobility Option and the Flow Mobility Sub-Options.

In case the LMA wants to convey flow-level information to the MAG, it MUST include in the FMI (or the PBA) a Flow Identification Mobility Option for all the flows that the MAG needs to be aware with flow granularity. Each Flow Identification Option MUST include a Traffic Selector Sub-Option including such flow-level information.

To remove a flow binding state at the MAG, the LMA simply sends a FMI (or PBA if it is in response to a PBU) message that includes flow identification options for all the flows that need to be refreshed, modified, or added, and simply omits those that need to be removed.

Note that even if a common set of prefixes is used, providing the MAG with flow-level information requires signaling to be exchanged in this case between the LMA and the MAG. This is done sending a FMI message (or a PBA if it is sent in response to a PBU).

## 4. Message Formats

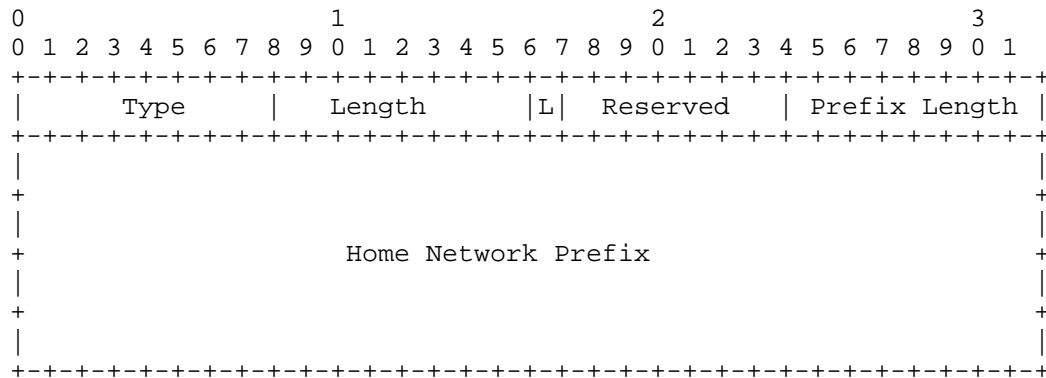
This section defines modifications to the Proxy Mobile IPv6 [RFC5213] protocol messages.

This specification requires implementation of UPN [RFC7077] and UPA [RFC7077] messages with the specific Notification Reason and Status Code values as defined by this document. This document does not require implementation of any other aspects of [RFC7077].

### 4.1. Home Network Prefix

A new flag (L) is included in the Home Network Prefix option to indicate to the Mobile Access Gateway whether the conveyed prefix has to be hosted on-link or not on the point-to-point interface with the mobile node. A prefix is hosted off-link for the flow mobility

purposes defined in this document. The rest of the Home Network Prefix option format remains the same as defined in [RFC5213].



Off-link Home Network Prefix Flag (L):

The Off-link Home Network Prefix Flag is set to indicate to the Mobile Access Gateway that the home network prefix conveyed in the option is not to be hosted on-link, but has to be considered for flow mobility purposes and therefore added to the Mobile Access Gateway routing table. If the flag is set to 0, the Mobile Access Gateway assumes that the home network prefix has to be hosted on-link.

#### 4.2. Flow Mobility Initiate (FMI)

The FMI message used in this specification is the Update Notification (UPN) message specified in [RFC7077]. The message format, transport and security consideration are as specified in [RFC7077]. The format of the message is specified in Section 4.1 of [RFC7077]. This specification does not modify the UPN message, however, it defines the following new notification reason value for use in this specification:

Notification Reason:

{IANA-1} - FLOW-MOBILITY. Request to add/refresh the prefix(es) conveyed in the Home Network Prefix options included in the message to the set of prefixes for which flow mobility is provided.

The Mobility Options field of an FMI MUST contain the MN-ID, followed by one or more Home Network Prefixes options. Prefixes for which flow mobility was provided that are not present in the message MUST be removed from the set of flow mobility enabled prefixes.

#### 4.3. Flow Mobility Acknowledgement (FMA)

The FMA message used in this specification is the Update Notification Ack (UPA) message specified in Section 4.2 of [RFC7077]. The message format, transport and security consideration are as specified in [RFC7077]. The format of the message is specified in Section 4.2 of [RFC7077]. This specification does not modify the UPA message, however, it defines the following new status code values for use in this specification:

Status Code:

0: Success.

{IANA-2}: Reason unspecified.

{IANA-3}: MN not attached.

When Status code is 0, the Mobility Options field of an FMA MUST contain the MN-ID, followed by one or more Home Network Prefixes options.

#### 5. Conceptual Data Structures

This section summarizes the extensions to Proxy Mobile IPv6 that are necessary to manage flow mobility.

##### 5.1. Multiple Proxy Care-of Address Registration

The binding cache structure of the local mobility anchor is extended to allow multiple proxy care-of address (Proxy-CoA) registrations, and support the mobile node use the same address (prefix) beyond a single interface and mobile access gateway. The LMA maintains multiple binding cache entries for an MN. The number of binding cache entries for a mobile node is equal to the number of the MN's interfaces attached to any MAGs.

This specification re-uses the extensions defined in [RFC5648] to manage multiple registrations, but in the context of Proxy Mobile IPv6. The binding cache is therefore extended to include more than one proxy care-of address and to associate each of them with a binding identifier (BID). Note that the BID is a local identifier, assigned and used by the local mobility anchor to identify which entry of the flow mobility cache is used to decide how to route a given flow.

BID-PRI	BID	MN-ID	ATT	HNP(s)	Proxy-CoA
20	1	MN1	WiFi	HNP1,HNP2	IP1 (MAG1)
30	2	MN1	3GPP	HNP1,HNP3	IP2 (MAG2)

Figure 6: Extended Binding Cache

Figure 6 shows an example of extended binding cache, containing two binding cache entries (BCEs) of a mobile node MN1 attached to the network using two different access technologies. Both of the two attachments share the same prefix (HNP1) and are bound to two different Proxy-CoAs (two MAGs).

## 5.2. Flow Mobility Cache

Each local mobility anchor MUST maintain a flow mobility cache (FMC) as shown in Figure 7. The flow mobility cache is a conceptual list of entries that is separate from the binding cache. This conceptual list contains an entry for each of the registered flows. This specification re-uses the format of the flow binding list defined in [RFC6089]. Each entry includes the following fields:

- o Flow Identifier Priority (FID-PRI).
- o Flow Identifier (FID).
- o Traffic Selector (TS).
- o Binding Identifier (BID).
- o Action.
- o Active/Inactive.

FID-PRI	FID	TS	BIDs	Action	A/I
10	2	TCP	1	Forward	Active
20	4	UDP	1,2	Forward	Inactive

Figure 7: Flow Mobility Cache

The BID field contains the identifier of the binding cache entry which packets matching the flow information described in the TS field

will be forwarded to. When a flow is decided to be moved, the affected BID(s) of the table are updated.

Similar to flow binding described in [RFC6089], each entry of the flow mobility cache points to a specific binding cache entry identifier (BID). When a flow is moved, the local mobility anchor simply updates the pointer of the flow binding entry with the BID of the interface to which the flow will be moved. The traffic selector (TS) in flow binding table is defined as in [RFC6088]. TS is used to classify the packets of flows based on specific parameters such as service type, source and destination address, etc. The packets matching with the same TS will be applied the same forwarding policy. FID-PRI is the order of precedence to take action on the traffic. Action may be forward or drop. If a binding entry becomes 'Inactive' it does not affect data traffic. An entry becomes 'Inactive' only if all of the BIDs are de-registered.

The mobile access gateway MAY also maintain a similar data structure. In case no full flow mobility state is required at the MAG, the Binding Update List (BUL) data structure is enough and no extra conceptual data entries are needed. In case full per-flow state is required at the mobile access gateway, it SHOULD also maintain a flow mobility cache structure.

## 6. Mobile Node considerations

This specification assumes that the mobile node IP layer interface can simultaneously and/or sequentially attach to multiple MAGs, possibly over multiple media. The mobile node MUST be able to enforce uplink policies to select the right outgoing interface. One alternative to achieve this multiple attachment is described in [I-D.ietf-netext-logical-interface-support], which allows the mobile node supporting traffic flows on different physical interfaces regardless of the assigned prefixes on those physical interfaces. Another alternative is configuring the IP stack of the mobile node to behave according to the weak host model [RFC1122].

## 7. IANA Considerations

This specification establishes new assignments to the IANA mobility parameters registry:

- o Handoff Indicator Option type: the value {IANA-0} has to be assigned from the "Handoff Indicator Option type values" registry defined in <http://www.iana.org/assignments/mobility-parameters/mobility-parameters.xhtml#mobility-parameters-9>.

- o Update Notification Reason: the value ({IANA-1}) has to be assigned from the "Update Notification Reasons Registry" defined in <http://www.iana.org/assignments/mobility-parameters/mobility-parameters.xhtml#upn-reasons>.
- o Update Notification Acknowledgement Status: values ({IANA-2} and {IANA-3}) have to be assigned from the "Update Notification Acknowledgement Status Registry". Since {IANA-2} and {IANA-3} are used in error messages, their values have to be greater than 128 from the range defined in <http://www.iana.org/assignments/mobility-parameters/mobility-parameters.xhtml#upa-status>.

## 8. Security Considerations

The protocol signaling extensions defined in this document share the same security concerns of Proxy Mobile IPv6 [RFC5213] and do not pose any additional security threats to those already identified in [RFC5213] and [RFC7077].

The mobile access gateway and the local mobility anchor MUST use the IPsec security mechanism mandated by Proxy Mobile IPv6 [RFC5213] to secure the signaling described in this document.

## 9. Authors

This document reflects contributions from the following authors (in alphabetical order).

Kuntal Chowdhury

E-mail: [kc@altiostar.com](mailto:kc@altiostar.com)

Sri Gundavelli

E-mail: [sgundave@cisco.com](mailto:sgundave@cisco.com)

Youn-Hee Han

E-mail: [yhhan@kut.ac.kr](mailto:yhhan@kut.ac.kr)

Yong-Geun Hong

E-mail: [yonggeun.hong@gmail.com](mailto:yonggeun.hong@gmail.com)

Rajeev Koodli

E-mail: [rajeevkoodli@google.com](mailto:rajeevkoodli@google.com)



Telemaco Melia

E-mail: telemaco.melia@googlemail.com

Frank Xia

E-mail: xiayangsong@huawei.com

## 10. Acknowledgments

The authors would like to thank Vijay Devarapalli, Mohana Dahamayanthi Jeyatharan, Kent Leung, Bruno Mongazon-Cazavet, Chan-Wah Ng, Behcet Sarikaya and Tran Minh Trung for their valuable contributions which helped generating this document.

The authors would also like to thank Juan-Carlos Zuniga, Pierrick Seite, Julien Laganier for all the useful discussions on this topic.

Finally, the authors would also like to thank Marco Liebsch, Juan-Carlos Zuniga, Dirk von Hugo, Fabio Giust and Daniel Corujo for their reviews of this document.

The work of Carlos J. Bernardos has been partially performed in the framework of the H2020-ICT-2014-2 project 5G NORMA.

## 11. References

### 11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<http://www.rfc-editor.org/info/rfc5213>>.
- [RFC5648] Wakikawa, R., Ed., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, DOI 10.17487/RFC5648, October 2009, <<http://www.rfc-editor.org/info/rfc5648>>.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, DOI 10.17487/RFC6088, January 2011, <<http://www.rfc-editor.org/info/rfc6088>>.

- [RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, DOI 10.17487/RFC6089, January 2011, <<http://www.rfc-editor.org/info/rfc6089>>.
- [RFC7077] Krishnan, S., Gundavelli, S., Liebsch, M., Yokota, H., and J. Korhonen, "Update Notifications for Proxy Mobile IPv6", RFC 7077, DOI 10.17487/RFC7077, November 2013, <<http://www.rfc-editor.org/info/rfc7077>>.

## 11.2. Informative References

- [I-D.ietf-netext-logical-interface-support]  
Melia, T. and S. Gundavelli, "Logical-interface Support for Multi-access enabled IP Hosts", draft-ietf-netext-logical-interface-support-13 (work in progress), February 2016.
- [RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <<http://www.rfc-editor.org/info/rfc1122>>.
- [RFC7222] Liebsch, M., Seite, P., Yokota, H., Korhonen, J., and S. Gundavelli, "Quality-of-Service Option for Proxy Mobile IPv6", RFC 7222, DOI 10.17487/RFC7222, May 2014, <<http://www.rfc-editor.org/info/rfc7222>>.

## Author's Address

Carlos J. Bernardos (editor)  
Universidad Carlos III de Madrid  
Av. Universidad, 30  
Leganes, Madrid 28911  
Spain

Phone: +34 91624 6236  
Email: [cjbc@it.uc3m.es](mailto:cjbc@it.uc3m.es)  
URI: <http://www.it.uc3m.es/cjbc/>

Network-Based Mobility Extensions  
(Netext)  
Internet-Draft  
Updates: 5213 (if approved)  
Intended status: Standards Track  
Expires: April 26, 2012

J. Korhonen  
Nokia Siemens Networks  
U. Nilsson  
TeliaSonera  
V. Devarapalli  
October 24, 2011

Service Selection for Mobile IPv6  
draft-korhonen-netext-rfc5149bis-00.txt

Abstract

In some Mobile IPv6 deployments, identifying the mobile node or the mobility service subscriber is not enough to distinguish between multiple services possibly provisioned to the said mobile node and its mobility service subscription. A capability to specify different services in addition to the mobile node identity can be leveraged to provide flexibility for mobility service providers on provisioning multiple services to one mobility service subscription. This document describes a Service Selection Mobility Option for both conventional Mobile IPv6 and Proxy Mobile IPv6 that is intended to assist home agents and local mobility agents to make a specific service selection for the mobility service subscription during the binding registration procedure. This specification updates RFC 5213.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 26, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Requirements . . . . .	4
3. Service Selection Mobility Option . . . . .	4
4. Processing Considerations . . . . .	5
4.1. Binding Cache Entry Lookup Considerations . . . . .	5
4.2. Mobile Node Considerations . . . . .	6
4.3. Home Agent and Local Mobility Agent Considerations . . . . .	6
4.4. Correspondent Node Considerations . . . . .	7
5. Security Considerations . . . . .	8
6. IANA Considerations . . . . .	8
7. References . . . . .	8
7.1. Normative references . . . . .	8
7.2. Informative references . . . . .	9
Authors' Addresses . . . . .	9

## 1. Introduction

Mobile IPv6 [RFC6275] can identify mobile nodes in various ways, including home addresses, Network Access Identifiers (NAIs) [RFC4282][RFC4283], and credentials suitable for the Internet Key Exchange Protocol version 2 (IKEv2) [RFC4877]. Proxy Mobile IPv6 [RFC5213] uses Home Network Prefix (HNP) and/or Mobile Node Identifier [RFC4283]. In some Mobile IPv6 deployments, identifying the mobile node or the mobility service subscriber via a Proxy Mobile IPv6 client [RFC5213] (hereafter, the mobile node and the Proxy Mobile IPv6 client are used interchangeably) is not enough to distinguish between multiple services possibly provisioned to the said mobile node and its mobility service subscription.

The capability to specify different services in addition to the mobile node identity can be leveraged to provide flexibility for mobility service providers to provide multiple services within the same mobility service subscription. For example:

- o Provide an enterprise data access for which the mobility service provider hosts connectivity and mobility services on behalf of the enterprise.
- o Provide access to service domains that are otherwise not accessible from public networks because of some mobility service provider's business reasons.
- o Provide simultaneous access to different service domains that are separated based on policies of the mobility service provider.
- o Enable easier policy and quality of service assignment for mobility service providers based on the subscribed services.
- o In the absence of a specifically indicated service, the home agent MUST act as if the default service, plain Internet access, had been requested. There is no absolute requirement that this default service be allowed to all subscribers, but it is highly RECOMMENDED in order to avoid having normal subscribers employ operator-specific configuration values in order to get basic service.

This document describes a Service Selection Mobility Option for (Proxy) Mobile IPv6 that is intended to assist home agents or local mobility agents to make specific service selections for the mobility service subscription during the binding registration procedure. The service selection may affect home agent or local mobility agent routing decisions, Home Address or Home Network Prefix assignment policies, firewall settings, and security policies. The Service

Selection option should be used in every Binding Update that makes a new registration to the home agent.

Some of the potential use-cases were listed earlier in this section. The general aim is better manageability of services and service provisioning from the point of view of both operators and service providers. However, it should be understood that there are potential deployment possibilities where selecting a certain service may restrict simultaneous access to other services from a user's point of view. For example, services may be located in different administrative domains or external customer networks that practice excessive filtering of inbound and outbound traffic.

## 2. Requirements

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 [RFC2119].

## 3. Service Selection Mobility Option

At most one Service Selection Mobility option SHOULD be included in any (Proxy) Binding Update message. If and only if the (Proxy) Binding Update message included the Service Selection Option, then the corresponding (Proxy) Binding Acknowledgement message SHOULD also contain the Service Selection option with the service name in the Identifier.

If the (Proxy) Binding Update message includes any authorization-related options (such as the Binding Authorization Data option [RFC6275]) or authentication related options (such as the Mobility Message Authentication option [RFC4285]), then the Service Selection option MUST appear before any mobility message authorization- or authentication-related options.

The Service Selection option SHOULD NOT be sent to a correspondent node. The mobile node cannot assume that the correspondent node has any knowledge about a specific service selection made between the mobile node and the home agent.

The Service Selection option has no alignment requirement as such.

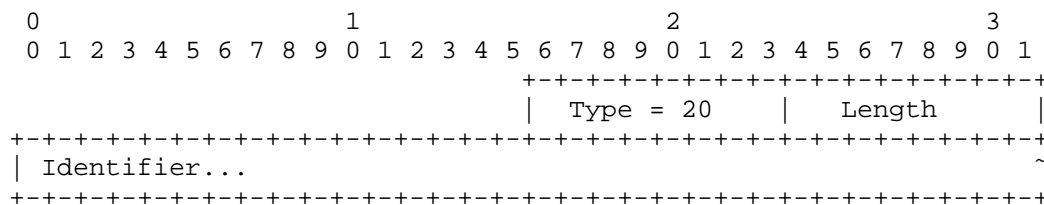


Figure 1: Service Selection Mobility Option

- o Type: 8-bit identifier set to 20 of the type of the skipable mobility option.
- o Length: 8-bit unsigned integer, representing the length of the Service Selection Mobility Option in octets, excluding the Option Type and Option Length fields. A value of zero (0) is not allowed.
- o Identifier: A variable-length encoded service identifier string used to identify the requested service. The identifier string length is between 1 and 255 octets. This specification allows international identifier strings that are based on the use of Unicode characters, encoded as UTF-8 [RFC3269], and formatted using Normalization Form KC (NFKC) as specified in [NFKC].

'ims', 'voip', and 'voip.companyxyz.example.com' are valid examples of Service Selection option Identifiers. At minimum, the Identifier MUST be unique among the home agents to which the mobile node is authorized to register.

[Discussion: Certain deployments encode the Identifier using RFC1035 domain name encoding. This should be described as well.]

## 4. Processing Considerations

### 4.1. Binding Cache Entry Lookup Considerations

Section 5.4.1 of [RFC5213] describes various Binding Cache Entry (BCE) lookup variations in the local mobility agent. Some existing Proxy Mobile IPv6 deployments have added the Service Selection option as one of the used BCE lookup keys. This implies that the Service Selection option SHOULD be included in all Proxy Binding Update messages, especially when the Home Network Prefix is not readily available.

[Discussion: Are there similar cases seen when using host based Mobile IPv6 or Dual-Stack Mobile IPv6?]

#### 4.2. Mobile Node Considerations

A mobile node or a Proxy Mobile IPv6 client MAY include, at most, one Service Selection Mobility Option into a (Proxy) Binding Update message. The option is used to identify the service to be associated with the binding registration and SHOULD only be included into the initial Binding Update message sent to a home agent. If the mobile node wishes to change the selected service, it is RECOMMENDED that the mobile node de-register the existing binding with the home agent before proceeding with a binding registration for a different service. The provisioning of the service identifiers to the mobile node or to the Proxy Mobile IPv6 client is out of the scope of this specification.

The placement of the Service Selection option is as follows: when present, this option MUST appear after the Mobile Node-Network Access Identifier (MN-NAI) option, if the MN-NAI option is present, and before any authorization- and authentication-related options. The Service Selection option can be used with any mobile node identification method such as a home address, an MN-NAI, and credentials suitable for IKEv2.

If the mobile node receives a (Proxy) Binding Acknowledgement with a Status Code set to SERVICE\_AUTHORIZATION\_FAILED and the mobile node has an existing binding with the Home Address or the Home Network Prefix used in the failed (Proxy) Binding Update message, the mobile node MUST delete the existing binding. If there is no existing binding, the mobile node proceeds as with any failed initial binding registration.

If the mobile node receives a (Proxy) Binding Acknowledgement with a Status Code set to MISSING\_OR\_UNKNOWN\_SERVICE the mobile node proceeds as with any failed initial binding registration. The mobile node SHOULD log the event as it is usually an indication of a configuration error.

#### 4.3. Home Agent and Local Mobility Agent Considerations

Upon receiving a (Proxy) Binding Update message with a Service Selection option, the home agent or the local mobility agent authenticates and authorizes the mobile node. If the home agent or the local mobility anchor supports the Service Selection and the Service Selection is required by the local policy, the home agent or the local mobility anchor MUST also verify that the mobile node is authorized for the service it included in the Service Selection option. The services the mobile node is authorized for SHOULD be part of the general mobile node subscription profile. If the mobile node is not authorized for the service, the home agent or the local



mobility agent MUST deny the registration and send a (Proxy) Binding Acknowledgement with a Status Code set to SERVICE\_AUTHORIZATION\_FAILED (151). If the (Proxy) Binding Update does not contain the Service Selection option or the indicated service is unknown, the home agent or the local mobility agent SHOULD deny the registration and send a (Proxy) Binding Acknowledgement with a Status Code set to MISSING\_OR\_UNKNOWN\_SERVICE (TBD).

If binding registration was successful in the home agent or the local mobility agent, then the (Proxy) Binding Acknowledgement SHOULD contain the Service Selection option with the service name in the Identifier.

The Service Selection option is used to assist the authorization and identifies a specific service that is to be authorized. The Service Selection option MAY also affect the Home Address or the Home Network Prefix allocation when, for example, used with the MN-NAI option. For example, for the same NAI there MAY be different Home Addresses or Home Network Prefixes depending on the identified service. Furthermore, the Service Selection option MAY also affect the routing of the outbound IP packets in the home agent or the local mobility agent depending on the selected service. The home agent MAY also apply different policy or quality of service treatment to traffic flows based on the selected service.

If the newly arrived (Proxy) Binding Update message with a Service Selection option indicates a change in the selected service, then the home agent MUST re-authorize the mobile node. Depending on the home agent or the local mobility agent policies, the services policies, Home Address or Home Network Prefix allocation policies, and the subscription policies, the home agent may or may not be able to authorize the mobile node to the new service. For example, the existing service and the new service could require different Home Network Prefixes. If the authorization fails, then the home agent or the local mobility agent MUST deny the registration, delete any binding with the existing Home Address or Home Network Prefix, and send a (Proxy) Binding Acknowledgement with a Status Code set to SERVICE\_AUTHORIZATION\_FAILED (151).

#### 4.4. Correspondent Node Considerations

Unless the correspondent node and the home agent share the same knowledge about mobility services, the Service Selection option is more or less useless information to the correspondent node. The correspondent node SHOULD silently ignore the Service Selection option in this case.

There are deployment cases where the home agent and a correspondent

node, for example, belong to the same administrative domain. In this case, it is possible that the correspondent node shares the same knowledge of the services as the home agent. Therefore, the correspondent node is, for example, able to provide service-based traffic handling to mobile nodes.

## 5. Security Considerations

The protection for the Service Selection Mobility Option depends on the service that is being identified and eventually selected. If the service selection information should not be revealed on the wire, (Proxy) Binding Updates and (Proxy) Binding Acknowledgements should use Encapsulating Security Payload (ESP) [RFC4303] in transport mode with a non-null encryption transform to provide message confidentiality.

## 6. IANA Considerations

A Mobile IPv6 Mobility Option type has been assigned for the following new mobility option from [RFC6275] "Mobility Options" registry. The mobility option is defined in Section 3:

Service Selection Mobility Option	is set to 20
-----------------------------------	--------------

A Mobile IPv6 registration denied by home agent Status Code has been assigned. The Status Code was allocated from the range 128-255:

SERVICE_AUTHORIZATION_FAILED	is set to 151
MISSING_OR_UNKNOWN_SERVICE	is set to TBD

## 7. References

### 7.1. Normative references

- [NFKC] Davis, M. and M. Durst, "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.0.0, October 2006.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

## 7.2. Informative references

- [RFC3269] Kermode, R. and L. Vicisano, "Author Guidelines for Reliable Multicast Transport (RMT) Building Blocks and Protocol Instantiation documents", RFC 3269, April 2002.
- [RFC4282] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.
- [RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.
- [RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.
- [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
- [RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

## Authors' Addresses

Jouni Korhonen  
Nokia Siemens Networks  
Linnoitustie 6  
FIN-02600 Espoo  
Finland

Email: jouni.nospam@gmail.com

Ulf Nilsson  
TeliaSonera Corporation  
Marbackagatan 11  
S-123 86 Farsta  
SWEDEN

Email: ulf.s.nilsson@teliasonera.com

Internet-Draft

Service Selection

October 2011

Vijay Devarapalli

Email: [dvijay@gmail.com](mailto:dvijay@gmail.com)



NETEXT WG  
Internet-Draft  
Intended status: Standards Track  
Expires: April 24, 2012

M. Liebsch  
NEC Laboratories Europe  
P. Seite  
France Telecom - Orange  
H. Yokota  
KDDI Lab  
J. Korhonen  
Nokia Siemens Networks  
S. Gundavelli  
Cisco  
October 22, 2011

Quality of Service Option for Proxy Mobile IPv6  
draft-liebsch-netext-pmip6-qos-00.txt

Abstract

This specification defines a new mobility option that can be used by the mobility entities in the Proxy Mobile IPv6 domain for exchanging the Quality of Service parameters associated with the subscriber flows. Specifically, the local mobility anchor in the home network can potentially send the QoS parameters to the mobile access gateway in the access network. This document also explains how the mobile access gateway in the access network can map the received QoS options to the access specific semantics, such as using 802.11e in case of IEEE 802.11 and apply it on the air interface.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 24, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the

document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions & Terminology . . . . .	5
2.1. Conventions . . . . .	5
2.2. Terminology . . . . .	5
3. Solution Overview . . . . .	6
4. Quality of Service Option . . . . .	7
5. QoS Mapping to 802.11e . . . . .	9
6. IANA Considerations . . . . .	10
7. Security Considerations . . . . .	11
8. Acknowledgements . . . . .	12
9. References . . . . .	13
9.1. Normative References . . . . .	13
9.2. Informative References . . . . .	13
Authors' Addresses . . . . .	15

## 1. Introduction

Mobile operators deploy Proxy Mobile IPv6 (PMIPv6) [RFC5213] to enable network-based mobility management for mobile nodes (MN). Users can access Internet Protocol (IP) based services from their mobile device by using different radio access technologies. Current standardization effort considers strong QoS classification and enforcement for cellular radio access technologies. QoS policies are typically controlled by a policy control function, whereas the policies are enforced by different gateways in the infrastructure, such as the LMA. Cellular radio access technology introduces the concept of a bearer. Each mobile node can have one or multiple bearers associated with its registration, each supporting different QoS characteristics. The bearer concept is not valid for alternative radio access technologies; however, these technologies specify their own concepts to enable QoS differentiation. Handover and IP Flow Mobility using alternative radio access technologies, such as IEEE802.16 and Wireless LAN according to the IEEE802.11 specification, are being considered by the standards [TS23.402], whereas inter-working between the cellular architecture to establish QoS policies in alternative access networks has not been focussed on so far.

In particular the Wireless LAN technology has been identified as promising alternative technology to complement cellular radio access. Since the 802.11e standard provides QoS extensions to WLAN, it is beneficial to apply QoS policies to the WLAN access, which enables QoS classification of downlink as well as uplink traffic between a UE and its LMA. Three functional operations have been identified to accomplish this:

- (a) Maintenance of QoS classification during a handover between cellular radio access and WLAN access by means of establishing QoS policies in the handover target access network,
- (b) mapping of QoS classes and associated policies between different access systems and
- (c) establishment of QoS policies for new data sessions/flows, which are initiated while using WLAN access.

This document specifies an extension to the PMIPv6 protocol, which enables the transport of established QoS descriptions between an LMA and the MAG by means of a QoS container option in case the QoS policy in the WLAN access is not under explicit control of a policy control system. The specified option allows association between IP session keys, such as a Differentiated Services Code Point (DSCP), and the expected QoS class for this IP session. Further handling of QoS



policies between the MAG and the WLAN Controller or WLAN Access Point is out of scope of this specification.

## 2. Conventions & Terminology

### 2.1. Conventions

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 [RFC2119].

### 2.2. Terminology

All the mobility related terms used in this document are to be interpreted as defined in the Proxy Mobile IPv6 specifications [RFC5213], [RFC5844], [RFC5845] and [RFC5846]. Additionally, this document uses the following abbreviations:

- o WLAN (Wireless Local Area Network) - A wireless network.
- o WTP (Wireless Termination Point): The entity that functions as the termination point for the network-end of the IEEE 802.11 based air interface from the mobile node. It is also known as the Wireless Access Point.
- o WLC (Wireless LAN Controller): The entity that provides the centralized forwarding, routing function for the user traffic. All the user traffic from the mobile nodes attached to the WTP's is typically tunneled to this centralized WLAN access controller.

### 3. Solution Overview

The following illustrates the scenario where the local mobility anchor in the cellular network provides QoS policy to the mobile access gateway in the WLAN access network. Other access technologies are also possible.

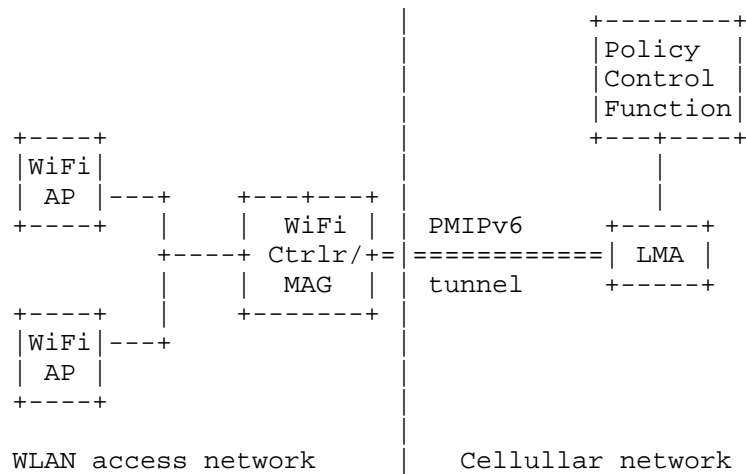


Figure 1: Scenario for QoS Interworking

#### 4. Quality of Service Option

A new option, Quality of Service option, is defined for using it in Proxy Binding Update (PBU) and Proxy Binding Acknowledgement (PBA) messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for providing QoS policies and information to the mobile access gateway.

The alignment requirement for this option is 4n.

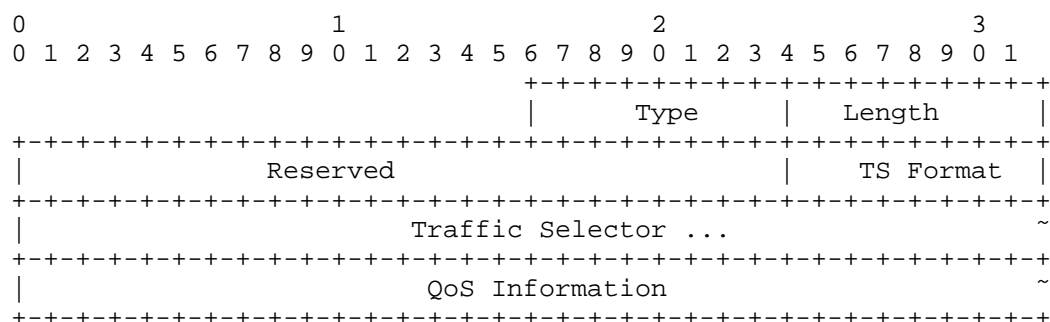


Figure 2: QoS Option

- o Type: To be assigned by IANA
- o Length: 8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields.
- o Reserved : This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.
- o TS Format: An 8-bit unsigned integer indicating the Traffic Selector Format. Value "0" is reserved and MUST NOT be used. The value of (1) is assigned for IPv4 Binary Traffic Selector [RFC6088].
- o TS Selector : variable-length opaque field for including the traffic specification identified by the TS format field. When the value of TS Format field is set to (1), the format that follows is the IPv4 Binary Traffic Selector specified in section 3.1 of

[RFC6088].

- o DSCP: An 6-bit unsigned integer indicating the code point value, as defined in [RFC2475] to be used for the flow.
- o QoS Information: one or more Type-Length-Value (TLV) encoded QoS parameters. The interpretation and usage of the QoS information is specific to the TLV. The QoS information MUST at least contain a DSCP value indicating the code point value, as defined in [RFC2475] to be used for the flow. [Discussion: which existing QoS definition to reuse? There are several around even in IETF space. RFC5624 is one potential as it already uses TLV encoding and is indirectly used by 23.402

## 5. QoS Mapping to 802.11e

This section discussed issues to be taken into account when mapping QoS parameters between different access technologies. TBD

## 6. IANA Considerations

This specification defines a new Mobility Header option, Quality of Service option. This option is described in Section 4. The Type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options [RFC6275].

## 7. Security Considerations

The quality of service option defined in this specification is for use in Proxy Binding Update and Proxy Binding Acknowledgement messages. This option is carried like any other mobility header option as specified in [RFC5213] and does not require any special security considerations. Carrying quality of service information does not introduce any new security vulnerabilities.



## 8. Acknowledgements

The author of this document thanks the members of the NETLMM working group for all the discussions related to this topic.

## 9. References

### 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5779] Korhonen, J., Bournelle, J., Chowdhury, K., Muhanna, A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server", RFC 5779, February 2010.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.
- [RFC6085] Gundavelli, S., Townsley, M., Troan, O., and W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", RFC 6085, January 2011.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

### 9.2. Informative References

- [I-D.liebsch-netext-pmip6-authiwbk] Gundavelli, S., Liebsch, M., and P. Seite, "PMIPv6 inter-working with WiFi access authentication", draft-liebsch-netext-pmip6-authiwbk-03 (work in progress), October 2011.
- [RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
- [RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

- [RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung,  
"Generic Routing Encapsulation (GRE) Key Option for Proxy  
Mobile IPv6", RFC 5845, June 2010.
- [RFC5846] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K.,  
and P. Yegani, "Binding Revocation for IPv6 Mobility",  
RFC 5846, June 2010.
- [RFC6224] Schmidt, T., Waehlich, M., and S. Krishnan, "Base  
Deployment for Multicast Listener Support in Proxy Mobile  
IPv6 (PMIPv6) Domains", RFC 6224, April 2011.
- [TS23.402] 3GPP, "Architecture enhancements for non-3GPP accesses",  
2010.

## Authors' Addresses

Marco Liebsch  
NEC Laboratories Europe  
Kurfuersten-Anlage 36  
Heidelberg D-69115  
Germany

Email: [liebsch@neclab.eu](mailto:liebsch@neclab.eu)

Pierrick Seite  
France Telecom - Orange  
4, rue du Clos Courtel, BP 91226  
Cesson-Sevigne 35512  
France

Email: [pierrick.seite@orange.com](mailto:pierrick.seite@orange.com)

Hidetoshi Yokota  
KDDI Lab  
2-1-15 Ohara  
Saitama, Fujimino 356-8502  
Japan

Email: [yokota@kddilabs.jp](mailto:yokota@kddilabs.jp)

Jouni Korhonen  
Nokia Siemens Networks  
Linnoitustie 6  
Espoo FI-02600  
Finland

Email: [jouni.nospam@gmail.com](mailto:jouni.nospam@gmail.com)

Sri Gundavelli  
Cisco  
170 West Tasman Drive  
San Jose, CA 95134  
USA

Email: [sgundave@cisco.com](mailto:sgundave@cisco.com)



NETLMM extensions [netext]  
Internet-Draft  
Intended status: Informational  
Expires: April 28, 2012

C. Perkins  
Tellabs  
B. Patil  
Nokia  
Oct 26, 2011

Optimizing IP Mobility Authentication with EAP  
draft-perkins-netext-eapbu-01.txt

Abstract

The Extensible Authentication Protocol (EAP) is commonly used for access authentication in many wireless networks. EAP methods often involve AAA servers to effect the required authentications; notifications about success or failure are then relayed back to a functional module in the access network known as the Network Access Server. The Binding Authentication Data option has been defined for enabling alternative methods for authentication in the context of Mobile IPv6, and there is a subtype allocated for AAA-based authentication methods such as EAP. However, some EAP methods require additional handling that requires specification not yet available in the existing documentation for the Binding Authentication Data option. This document provides the required specification for at least some very widely deployed EAP methods. In many situations requiring the use of EAP, this enables much faster operation for Mobile IPv6 tunnel redirection to a wireless device's new care-of address by avoiding having to do multiple authentications.

Status of This Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 28, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Problem Statement . . . . .	3
3. Proposed Solution . . . . .	4
3.1. Example . . . . .	4
4. EAP subtype for Binding Authentication Data . . . . .	5
5. Binding Acknowledgement Authentication Data option . . . . .	5
6. Example of use with EAP-AKA . . . . .	6
7. Security Considerations . . . . .	7
8. IANA Considerations . . . . .	7
9. References . . . . .	7
9.1. Normative References . . . . .	7
9.2. Informational References . . . . .	8

## 1. Introduction

The Extensible Authentication Protocol (EAP) [RFC3748] is commonly used for access authentication in many wireless networks. EAP methods often involve AAA servers to effect the required authentications; notifications are then relayed back to a functional module in the access network known as the Network Access Server. For Mobile IPv6 [RFC6275], the Binding Authentication Data option [RFC4285] has been defined for enabling alternative methods for authentication, and a subtype has been allocated for AAA-based authentication methods such as EAP. However, some EAP methods require additional handling that requires specification not yet available in the existing documentation for the Binding Authentication Data option. This document provides the required specification for at least some very widely deployed EAP methods. In many situations requiring the use of EAP, this enables much faster operation for Mobile IPv6 tunnel redirection to a wireless device's new care-of address.

## 2. Problem Statement

Mobile IPv6 [RFC6275] requires the mobile node (MN) to authenticate with its assigned home agent. Establishing an IPsec SA is accomplished after the MN has been authenticated. EAP methods may be used within IKEv2 to authenticate the MN and then establish the MN's IPsec security association (SA). The authentication and establishment of the IPsec SA is required in addition to access network authentication. Most networks require a user/device to authenticate prior to being connected to the network. This results in the MN having to perform two authentications. The MN has to first perform access authentication and then authenticate again for a second time with the home agent to establish the IPsec SA. This causes significant delay in the MN being registered with the HA. It should be noted that when the MN moves to a different access network, access network authentication is typically performed. However, when the IPsec SA already exists, that SA only needs to be updated with the changed end-point. This can be achieved by setting the 'K' bit in the binding update sent from the new care-of-address.

In the case of network based mobility, i.e Proxy Mobile IPv6 [RFC5213] the Mobility Access Gateway (MAG) performs registration with the Local Mobility Agent (LMA) following access authentication. The MAG receives confirmation from a AAA server if the MN is authorized for mobility service and only after that does it send the proxy binding update to the LMA.

Combining access authentication with mobility authentication results in an optimization and faster connectivity. How to optimize or



combine the access authentication with the authentication required for obtaining mobility service is the problem dealt with in this document.

### 3. Proposed Solution

The proposal contained in this I-D is to combine access authentication with Mobile IPv6 authentication. As a result it saves at least one authentication sequence and hence speeds up the process of sending and receiving packets via the home agent or LMA.

EAP is commonly used for access authentication. Many of the EAP authentication methods interact with a AAA server which contain the credentials of the user. The NAS element in an access network is essentially a AAA relay entity. The proposal contained in this document aims to utilize the information available to the NAS from the access authentication phase to perform Mobile IP authentication as well. The extensions needed to EAP and the Mobile IP signaling are described in the following sections.

The basic idea is to route the access authentication signaling messages via the HA/LMA and thereby perform authentication and registration in a single transaction. The HA acts as a relay entity in the access authentication procedure and is aware of the result of the authentication procedure and can act on it by updating the binding cache.

#### 3.1. Example

The figure below shows an example of the solution which combines access authentication with mobility registration. In the figure the MN is presumed to already have a binding at the HA. Additionally the same scenario can be considered applicable to the network based mobility solution in which case the MAG routes the access authentication messages via the LMA.

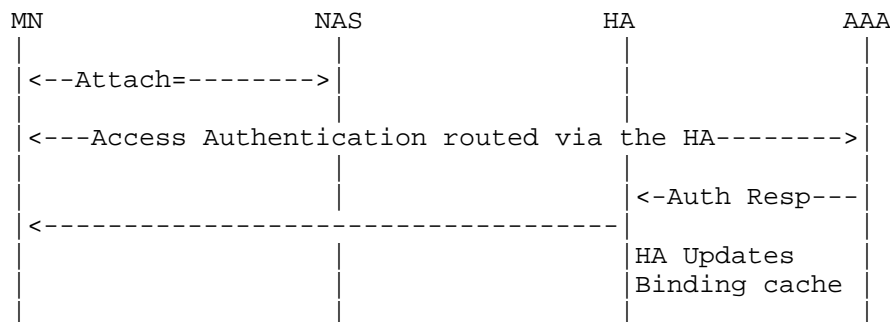
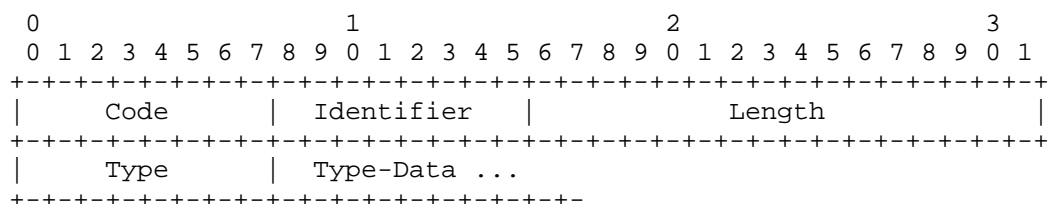


Figure 1: Example of combined authentication and registration

## 4. EAP subtype for Binding Authentication Data

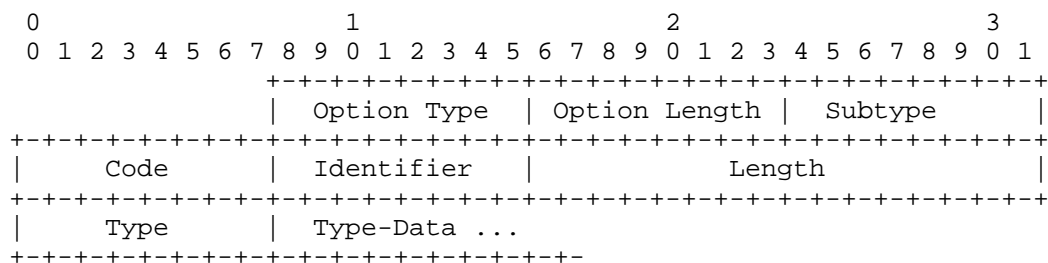
This specification defines a new subtype, called the EAP Authentication Data [EAPAD] subtype, for the Binding Authentication Data suboption for Mobile IPv6. The EAPAD subtype has the following format, which is identical to the EAP message format:



Please consult the EAP specification [RFC3748] for details about these header fields.

## 5. Binding Acknowledgement Authentication Data option

The Binding Acknowledgement Authentication Data option [BACKAD] is specified to enable the EAP method to return data from the AAA server back to the Authenticator and the Peer as may be required by the EAP method specification. The nature of the data returned in the BACKAD depends on the method. The EAP message is of type EAP Success or EAP Failure.



The Subtype for the Binding Acknowledgement Authentication Data option is 0, for EAP methods. There is no need for the SPI field. The Type-Data is the EAP method-specific data. Since this option appears in the Binding Acknowledgement (or Proxy Binding Acknowledgement) message, the Code will either correspond to EAP-Success or EAP-Failure.

## 6. Example of use with EAP-AKA

The following figure shows how to use the new Binding Authentication Data subtype along with the new Binding Acknowledgement Authentication Data subtype with EAP-AKA [RFC4187]. A very similar procedure will also work for EAP-AKA' [RFC5448].

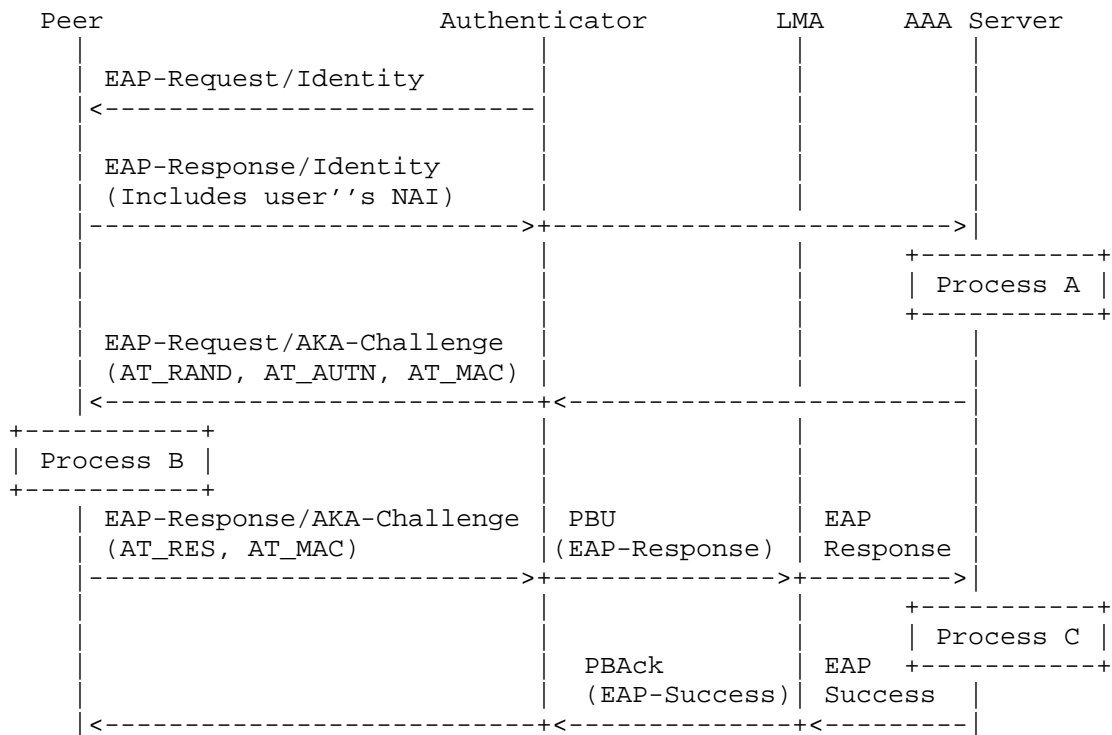


Figure 2: Use of EAPAD and BackAD in EAP-AKA Authentication

where:

Process A

means "Server runs AKA algorithms, generates RAND and AUTN."

Process B

means "Peer runs AKA algorithms, verifies AUTN and MAC, derives RES and session key"

## Process C

means "Server checks the given RES, and MAC and finds them correct."

## 7. Security Considerations

This document introduces a new subtype for the Binding Authentication Data of Mobile IPv6. The security characteristics for the authentication data are exactly those of the base EAP method which defines the data fields and security parameters for the new subtype.

This document specifies the Binding Acknowledgement Data option, which is a new option for the Binding Acknowledgement message of Mobile IPv6. The security characteristics for the new option are exactly those of the base EAP method which defines the data fields and security parameters for the new option. The Mobile-Home Authentication extension is still also required for the Binding Acknowledgement, but additional security features and notifications may be included in the EAP method data defining the contents of the new option. PMIP uses the same message format for BACK, and the new option works in the same way whether or not the 'P' bit is set.

## 8. IANA Considerations

This document requires allocation of a new subtype for the Binding Authentication Option of Mobile IPv6.

This document specifies the Binding Acknowledgement Data option, which is a new option for the Binding Acknowledgement message of Mobile IPv6.

## 9. References

## 9.1. Normative References

- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.
- [RFC4285] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

## 9.2. Informational References

- [RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, January 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, May 2009.

## Authors' Addresses

Charles E. Perkins  
Tellabs

Phone: +1-408-970-6560  
EMail: charliep@tellabs.com

Basavaraj Patil  
Nokia  
6021 Connection Drive  
Irving, TX 75039  
USA

EMail: basavaraj.patil@nokia.com



Network Working Group  
Internet-Draft  
Expires: December 9, 2012

B. Sarikaya  
F. Xia  
Huawei  
June 7, 2012

PMIPv6 Multihoming Support for Flow Mobility  
draft-sarikaya-netext-fb-support-extensions-02

Abstract

This document specifies extensions to Proxy Mobile IPv6 (PMIPv6) for flow mobility support. Binding cache, binding update list and home network prefix option are slightly extended to allow indicating the home interface and other interfaces.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on December 9, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Terminology . . . . .	3
3. Problem Statement . . . . .	4
4. Multihoming Case . . . . .	5
5. LMA Operation . . . . .	5
5.1. Extensions to Binding Cache Entry . . . . .	5
6. MAG Operation . . . . .	6
6.1. Extensions to Binding Update List Entry Data Structure . .	7
7. Message Formats . . . . .	7
8. Security Considerations . . . . .	8
9. IANA considerations . . . . .	8
10. Acknowledgements . . . . .	8
11. References . . . . .	8
11.1. Normative References . . . . .	8
11.2. Informative references . . . . .	9
Authors' Addresses . . . . .	10



## 1. Introduction

In Mobile IPv6 [RFC6275] multi-homing is supported efficiently due to the use of home address. Mobile node uses its home address as the source address and all incoming traffic is directed to the home address (HoA). When multiple interfaces are concurrently active the home agent (HA) has to decide how to route incoming packets to different active interfaces. HA does this based on the flow bindings. MN has to register its active flows with the HA and HA keeps flow binding entries for each HoA. HA then forwards packets to one of the care-of addresses of an active interface after matching it with an ordered list of flow bindings.

Proxy Mobile IPv6 [RFC5213] lacks a similar mechanism because each active interface is treated separately and a different binding cache entry is created. This document proposes changes necessary to the local mobility anchor (LMA) behaviour so that flow mobility can seamlessly be supported in PMIPv6. The changes to the mobile node considered in [I-D.ietf-netext-logical-interface-support] are also needed to complement our solution on the host side.

## 2. Terminology

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].

The terminology in this document is based on the definitions in [RFC5213], [RFC6089] in addition to the ones specified in this section:

Single-Radio MN: Consider MN with two interfaces. These interfaces are implemented in such a way that MN can keep one radio module (interface) active at a given time.

Dual/multiple-Radio MN: Consider MN with two interfaces. These interfaces are implemented in such a way that both radio modules can receive and transmit simultaneously.

Inter-technology handover: Sometimes called vertical handover. A multi-homed MN communicates with one interface at any time to conserve power. Each interface can support different access technology. Inter-technology handover occurs when MN moves out of coverage of one technology and moves into the coverage area of another technology which will result in switching of the communicating interface on MN  
[I-D.ietf-netext-logical-interface-support].

### 3. Problem Statement

In base Proxy Mobile IPv6 when MN connects simultaneously with multiple interfaces each interface is treated independently and MN uses different source addresses when sending packet over these interfaces [RFC5213]. However in case of flow mobility, MN itself or LMA might wish to move one flow from one interface to the other. When a flow is moved from interface A to interface B, MN has to stop sending packets on interface A, i.e. it should set the source address to an address based on HNPs assigned to interface B. Forcing an MN to do this after a flow is moved is difficult currently and is one of the problems PMIPv6 flow mobility is facing.

The solution for this is to let MN always use a source address from HNPs assigned to its home interface. When multiple interfaces are active, incoming packets can be directed to different active interfaces based on flow state established at LMA.

In based Proxy Mobile IPv6 LMA treats each interface independently of the other interface(s) MN may have and tries to provide mobility support for each interface. LMA does not manage bindings from different interfaces of the mobile node in an integrated fashion. So LMA can not be in control of moving the flows in between interfaces.

The solution to this is to modify the way the binding cache is managed. Instead of creating an independent mobility session for each interface, the bindings from each interface are kept together so that the flows can be moved among interfaces. The extensions to the base protocol needed for this should be minimal.

When MN does an inter-technology handover, the new MAG sends a Proxy Binding Update (PBU) message to the local mobility anchor (LMA) to register the new proxy care-of address. In the PBU, MAG sets the access technology type (ATT) and handoff indicator (HI) values. If ATT is different from the one stored in the existing binding cache entry for this MN and if HI is set to 2 (Handoff between two different interfaces of the mobile node), LMA concludes that an inter-technology handover happened and assigns the same home network prefix(es) to MN which enables IP session continuity.

Setting the handoff indicator correctly is also not so easy. Most MAGs would tend to set HI to 1 (Attachment over a new interface) which would result in LMA setting new prefix(es) to MN and creating a new binding cache entry and allocating a new mobility session for this new interface. This behaviour as described in Section 5.4 of [RFC5213] needs to be changed.

#### 4. Multihoming Case

When there is attachment over a new interface (HI value received in the Binding Update from MAG is 1) LMA creates a new binding cache entry and assigns the flag "S" defined in Section 5.1 to all home network prefixes assigned to this interface. Also the corresponding value is set to the (H) flag of the home network interface option defined in Section 7 in the binding acknowledgement sent to MAG. LMA MUST also include the home network prefixes with "H" flag in the BA message. This should enable MN continue to send packets with source addresses selected from HNPs with "H" flag on.

The new binding cache entry does not create a new mobility session. The entry is considered as a pointer to another binding the same MN has with LMA. MN may have as many such binding entries as it has active interfaces. These secondary binding cache entries are refreshed regularly by MAGs sending BUs. MAG MUST include HNPs both with "H" and "S" flags in the BU message. LMA refreshes the binding cache entry for the interface with only "S" flag.

#### 5. LMA Operation

When LMA receives a Binding Update message which contains Handoff Indication set to a value of 1 LMA MUST create a new binding cache entry and assign new home network prefixes for this interface. In the binding cache entry these HNPs MUST be flagged with a value of 0 representing "S". This binding cache entry becomes part of the binding cache entry that contains home network prefixes with "H" flag. "H" and "S" flags are as defined in Section 5.1.

LMA sends home network prefixes assigned to the new interface in the Binding Acknowledgement message. LMA MUST also set the (H) Flag in HNP option to 0. In the same BA message, LMA MAY also send home network prefixes whose (H) flag is set to 1 in the same BA.

The modifications specified in this document allow a mobile node to have a single interface connected at a given moment and that interface has prefixes assigned an "S" flag, i.e. the binding with the home interface may have expired. In this case LMA MUST also store the home network prefixes with "H" flag in the binding cache entry.

##### 5.1. Extensions to Binding Cache Entry

One flag associated with the following binding cache entry: list of IPv6 home network prefixes assigned to the mobile node's connected interface and prefix length. The flag is set to 1 representing "H"

if the connected interface is the home interface and flag is set to 0 representing "S" if the connected interface is not the home interface but it is one of the secondary interfaces.

The prefixes assigned after the very first PBU is received for this MN are assigned the "H" flag. The handoff between two different interfaces does not require the prefixes to be changed in order to allow session continuity. Because of this the flag (of "H" or "S") associated with the prefixes stays the same.

This specification also brings the change that binding cache entries for the same MN-Identifier are considered together. The number of entries is equal to the number of active interfaces of MN. If there is a single entry it is assumed that the flag value is "H", otherwise the prefixes with "H" flag should also be stored in the binding cache entry.

For an incoming packet, the destination address MUST be selected from the set of prefixes with "H" flag, i.e. MN always sends non-local packets with source address assigned from HNPs of its home interface. LMA decides to which interface to route this packet by consulting the flow mobility cache [I-D.ietf-netext-pmipv6-flowmob], similar to the case in Mobile IPv6 [RFC6089]. The packet will be matched against the flow descriptions [RFC6088] in the flow mobility cache and Proxy-CoA of the matching entry will be determined. Next, binding cache entry for this MN will be searched and the packet will be directed to the MAG to which the matching interface is connected.

## 6. MAG Operation

When MAG detects an attachment over a new interface it sets Handoff Indicator field to 1 as described in [RFC5213] in the Binding Update message that it sends to LMA.

MAG MUST store home network prefixes it receives in Binding Acknowledgement message from LMA together with the flag in the binding update list entry. If the flag is "S" MAG MUST also store all home network prefixes in the BA message whose flag is "H" in the corresponding binding update list entry. There will be a maximum of two sets of HNPs for each MN if the MAG is not connected to the home interface.

MAG receives packets from LMA, decapsulates them and searches the binding update list to find the corresponding entry (with the "H" flag) and sends them to the MN with the corresponding "S" flag.

### 6.1. Extensions to Binding Update List Entry Data Structure

A flag associated with the following binding update list entry: list of IPv6 home network prefixes assigned to the mobile node's connected interface the corresponding prefix length. The flag is set to 0 representing "H" if the connected interface is the home interface and is set to 1 representing "S" if the connected interface is not.

MAG MUST also store the home network prefixes with flag "H" in addition to the prefixes associated with the connected interface if the flag of the home network prefix assigned to the connected interface is "S". MAG determines these flag values from the home network prefix option's (H) flag.

## 7. Message Formats

Home Network Prefix Option defined in [RFC5213] is modified to include a flag to indicate if home network prefixes are associated with "H" flag or "S" flag in the binding cache entries.

This specification extends the Home Network Prefix Option with a new flag. The flag is shown and described below. All other fields are as described in [RFC5213].

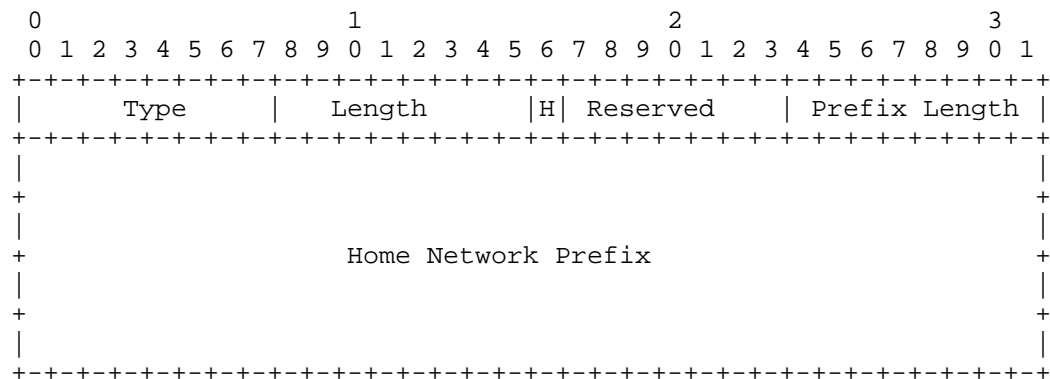


Figure 1: Home Network Prefix Option

### H Flag

This flag is set to 1 when this prefix is assigned to a secondary interface of the mobile node, i.e. when the binding cache entry for this HNP has "S" flag set. This flag is set to 0 when this prefix is assigned to the firstly connecting or the only connected interface of the mobile node, i.e. when the binding cache entry

for this HNP has "H" flag set.

## 8. Security Considerations

This document does not define any new security issues. PMIPv6 security procedures apply.

## 9. IANA considerations

IANA is requested to add the H Flag into the reserved field in Home Network Prefix Option defined in Section 8.3 in [RFC5213] as the first bit, i.e. Bit number 16 and change the Reserved (R) field as follows:

This 7-bit field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

## 10. Acknowledgements

The authors thank Hidetoshi Yokota who provided valuable comments.

## 11. References

### 11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K.,

and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T.,  
and K. Nagami, "Multiple Care-of Addresses Registration",  
RFC 5648, October 2009.

#### 11.2. Informative references

[I-D.ietf-netext-pmipv6-flowmob]  
Cano, C., "Proxy Mobile IPv6 Extensions to Support Flow  
Mobility", draft-ietf-netext-pmipv6-flowmob-03 (work in  
progress), March 2012.

[I-D.ietf-netext-logical-interface-support]  
Melia, T. and S. Gundavelli, "Logical Interface Support  
for multi-mode IP Hosts",  
draft-ietf-netext-logical-interface-support-05 (work in  
progress), April 2012.

Authors' Addresses

Behcet Sarikaya  
Huawei  
5340 Legacy Dr.  
Plano, TX 75074

Email: sarikaya@ieee.org

Frank Xia  
Huawei  
Nanjing, China

Phone:  
Email: xiayangsong@huawei.com





NETEXT Working Group  
Internet-Draft  
Intended status: Informational  
Expires: April 24, 2012

T. Tian  
W. Yan  
Y. Wei  
ZTE  
October 22, 2011

Problem Statement of Flow Mobility Triggering  
draft-tian-netext-flow-mobility-trigger-ps-00

Abstract

This document is a contribution draft which summaries the potential approaches for flow mobility triggering and gives analysis of these trigger methods based on the long-standing active discussion in the mailing list, which aims to achieve a common consensus on the issues and the working scope related to flow mobility trigger in Netext WG.

Requirements Language

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[RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 24, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents

(<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Flow mobility trigger Summary . . . . .	3
2.1. Host-based triggering . . . . .	3
2.2. Network-based triggering . . . . .	5
3. Other main issues . . . . .	6
3.1. MN capability discovery . . . . .	6
3.2. Policy synchronization . . . . .	7
4. Discussion for Decision . . . . .	8
5. IANA Considerations . . . . .	9
6. References . . . . .	9
6.1. Normative References . . . . .	9
6.2. Informative References . . . . .	9
Authors' Addresses . . . . .	10

## 1. Introduction

With the rapid growth of wireless network technology and the terminal technology, a mobile node that is equipped with various access modules has the ability to simultaneously connect to different access technologies. A definition of flow mobility is quoted from the mailing list: "In the context of Proxy MIP6 is the switching of a flow by the LMA from MAGx to MAGy when the MN is attached to the LMA via multiple interfaces through different MAGs." Flow mobility is now becoming an important issue to increase the availability of different network resources and to help to provide better user experience.

There has been lot of work focusing on supporting flow mobility in Netext WG, i.e., [I-D.ietf-netext-logical-interface-support], the "logical interface" defined in this draft makes all physical interfaces to hide from the network layer and above, which is a fundamental dependency for flow mobility. Flow mobility depends on the existence of a logical interface on the host.

"Proxy Mobile IPv6 Extensions to Support Flow Mobility"  
[I-D.ietf-netext-pmipv6-flowmob-ob], this draft defines PMIP6 extensions to support follow mobility over multiple physical interfaces. It describes how LMA excuses flow mobility based on the enhanced PMIP6 protocol;

"Multi-access Indicator for Mobility"  
[I-D.koodli-netext-multiaccess-indicator], this draft defines a new EAP attribute to indicate to the network the MN's capability of simultaneous multil-access and supporting of flow mobility.

But without making the trigger for flow mobility clear, the execution of flow mobility will be a castle in the air. The triggering issue has been discussed actively in the mailing list for a long time. This document summarizes the main ideas, the related analysis and relevant issues based on the discussion in mailing list, which aims to achieve a common consensus and make progress for the further work.

## 2. Flow mobility trigger Summary

The trigger solutions are broadly grouped into two categories, namely: Host-based triggering and Network-based triggering.

### 2.1. Host-based triggering

## 1. L3-signaling trigger

An example of L3-signaling solution is proposed in [I-D.ietf-netext-logical-interface-support] section 7.3 regards: "As an example of mobile-based triggers, the LMA could receive input (e.g. by means of a layer 2.5 function via L3 signaling [RFC5677]) from the MN detecting changes in the mobile wireless environment (e.g. weak radio signal, new network detected, etc.). Upon receiving these triggers, the LMA can initiate the flow mobility procedures. For instance, when the mobile node only supports single-radio operation (i.e. one radio transmitting at a time), only sequential (i.e. not simultaneous) attachment to different MAGs over different media is possible. In this case layer 2.5 signaling can be used to perform the inter-access technology handover and communicate to the LMA the desired target access technology, MN-ID, Flow-ID and prefix."

However, specifying a MN/host to a MAG signaling related to flow mobility at layer 3 has been put explicitly out of the charter of this WG.

## 2. Explicit flow trigger

Another host-based solution was proposed in the mailing list: "The MN can decide (based on policies) to change the flow and send packets over a new interface. The MAG would forward the packet with no problem and upon receiving this packet the LMA would implicitly know that the MN has performed a flow movement (again, based on policies). At this point the LMA would just need to change its routing table accordingly and start sending packets for this flow over the new interface (similar rule to the one already specified for the mobile)."

This is a lightweight host-centric solution which is suitable for the cases that the MN sends the UL flow and the MN itself decides and triggers the flow movement. No extensions to the existing RFC 5213 are needed, i.e. neither the modification of data structures nor the addition of new signaling. But for the case that the network decides the flow mobility based on the network conditions, this solution is not suitable.

In 3GPP the work TS 23.261 [TS23261] of host-based model for flow mobility based on MIP6 has been solved, which specifies the Stage 2 system description for IP flow mobility between a 3GPP and a WLAN. As PMIP6 is a network-based mobility support protocol and it does not require MNs to be involved in the mobility support signaling, and there is also requirement to enable network

controlled flow mobility, for example, to release the traffic pressure in the network based on network load conditions, the preference is to develop a network centric (i.e. MAG/LMA entities) flow mobility solution.

## 2.2. Network-based triggering

### 1. L2-signaling trigger (MAG trigger)

This approach is when a MN attaches to a new MAG, the MN uses the L2 signaling to indicate the attachment is for flow mobility, for example, with a new HI=FM value, then the MAG sends the PBU with HI=FM, and the LMA updates an existing session with the new interface and the new MAG. The old and new prefixes are shared for the session.

This approach keeps the existing RFC 5213[RFC5213] model. Advantage of this approach is that, with indication of the specific L2 signaling, the network will be able to have knowledge of the MN's capability of supporting flow mobility. Concern is that, the L2 signaling needs to be extended for flow mobility trigger purpose. However, L2 signaling is specified for specific link types in relevant SDOs, the extension work of specific L2 signaling is out of scope of IETF and should be done in other relevant SDOs. For example, 3GPP is one of the important potential customers; 3GPP owns the specific L2 used to access their system. It is possible that 3GPP may need to add extensions to make this solution work in their architecture, but even though, relying on modification of specific layer 2 protocols will let the solution only works with some technologies. As we are not chartered to come up with the 3GPP-only solution, both the cases when either new L2 signaling is available or L2 signaling is unavailable need to be included in our solution.

### 2. LMA trigger

This approach is now regarded as a pure network-centric trigger based on the network condition, and it is just up to the LMA that decides and triggers the flow mobility without involvement of the MN. Lots of concerns about this approach are raised on the mailing list.

Firstly, how does the network know whether the MN has the capability to support flow mobility or not. This issue will be discussed detailed in the later section.

Secondly, how does the LMA actually decide to route flows on one access or the other? This is another major concern raised on the mailing list is related to how flow mobility would work when an MN attaches to a wifi access and the LMA switches a flow(s) to the MAG serving the MN via that wifi. In cellular networks, the handovers are controlled by the network because the network always knows the link condition of the MN by the measurement reports provided by the MN. But in WLAN there is a huge difference. Others than the MN measurement report mechanism in the cellular network, the MN has no way of report the LMA about its connectivity/link status , e.g. the congestion, or other state of its attachment to a AP. Flows forwarded by the LMA to the MN via the wifi-MAG could be dropped if the MN has moved out of that wifi coverage or the link is congested. There are no existing protocols which can be used for the external interface between LMA and MN, the LMA only knows that the MN has attached via a MAG. It also mentioned in the mailing list that, there are solutions which allow the owner of the WLAN to know of the quality and status of the network. Even though, the lack of providing relevant information to the LMA is still an issue.

One view in the mailing list thought the intent of this work is on specifying how the traffic associated with a session is switched to an alternate MAG, the above points are outside the scope. But without knowing the information and feedback from the MN side, the LMA is hard to make a correct decision for flow mobility.

Thirdly, where does the LMA would receive the policies related to flow mobility, should there be a solution to have policies in the LMA, should the policy synchronization between LMA and MN be considered? This will be discussed in the later section.

### 3. Other main issues

#### 3.1. MN capability discovery

The network only offers flow mobility to the MN that indicates its support for the feature. Actually the capability discovery can be achieved by layer2, 3 or even 7, but within the restriction of current charter of this work, if this should be done, it has to be done at layer 2.

Following assumptions are summarized in the mailing list:

1. MN capabilities are known;

assumption that the indication of capability is achieved by Layer 3 or Layer 7 which is out of scope here;

2. Possible existence of layer 2 signaling to provide hints (HI = Flow Mobility);

"Multi-access Indicator for Mobility"[I-D.koodli-netext-multiaccess-indicator] provides one way to achieve this; it defines a new EAP attribute which can be used to indicate the MN's capability during the EAP-AKA procedure. The purpose of the multi-access indicator ID is twofold: to enable the MN to indicate its capability and willingness for flow mobility (through the AT\_MA\_IND attribute). Second, to enable AAA to authorize the user for flow mobility. So, it's the MN which is indicating the device capability, and the AAA providing the authorization for the flow mobility service.

3. Possible non-existence of layer-2 signaling to provide hints (HI = Unknown)

### 3.2. Policy synchronization

There is a need of policy synchronization between the MN side and the network side. In [I-D.ietf-netext-pmipv6-flowmob-ob] , it states that:

"As described in[I-D.ietf-netext-logical-interface-support] , there should be a local policy in place that ensures that packets are forwarded coherently. This SHOULD be enforced by the logical interface engine [I-D.ietf-netext-logical-interface-support]. For unidirectional outbound communications, there SHOULD also be a policy at the mobile node defining which physical interface is used to send the traffic. For bidirectional outbound communications, there SHOULD be also such a policy, but its content must be consistent with the policy at the network-side (the details about how this consistency is ensured are out of the scope of this document)."

The simplest way to do is to statically configure the same policies on the MN and the LMA, but this is not flexible and not unrealistic in the practical deployment.

For dynamic configuration of policies, ANDSF defined by 3GPP is proposed in the mailing list as one solution to help to achieve policy synchronization between the MN and the network. ANDSF is designed specific to be a MN-centric solution where policies are



provisioned in the MN and the MN decides which network technologies and access networks it needs to connect to, under what conditions, and which IP traffic needs to be routed on such accesses. ANDSF has the interface with MN, for example the push model in 3GPP, ANDSF can send SMS to UE via S14 interface to request MN to update its policy. The same policies in ANDSF delivered to the MN can be also offered to the network nodes, i.e. the MAG/LMA. There is neither MN-AR interface nor ANDSF-MAG/LMA interface in the existing specifications. To support this ANDSF approach, additional interfaces may be needed. Alternatively, policies delivery from PCRF to MAG/LMA is another suggestion. However, PCRF does not have the information to tell the LMA which policies are used for flow mobility, if the solution may be used, enhancement of PCC functionality will be needed.

Moreover, a scenario raised on the mailing list shows that, ANDSF policies may be based also on location of the MN. For example the MN should prefer WLAN only in a given location. When the MN is attached over WLAN there is no way for the LMA to verify the location of the MN and therefore to verify MN actions based on policies. In this case, this is another reason for the LMA to know the information of MN in WLAN. The lack of MN-AR interface is surely an issue for supporting some flow policies.

#### 4. Discussion for Decision

The feature of no involvement of the MN of PMIP6 decides it would not have the same degree of control in terms of handover flows or the granularity compared with MIP6. The PMIP6 based flow mobility would be applicable in deployments which leverage network based mobility, and the scope of this work is NOT intended to provide the same set of capabilities that exist in the host-based flow mobility solution.

Could we work on the flow mobility trigger in this WG? If the solution is related to the common protocol (e.g. EAP) which is used in specific L2 signaling, could it be discussed in this WG? There is strong reason for the LMA to obtain the information of MN in access networks, such as connectivity status, link characteristics and even the location information, either for the LMA to make a correct decision for flow mobility or to support some complex flow policies. Where could the LMA get the policies for flow mobility, and how the policies are synchronized with the MN's, are these issues still needed to be considered?

One option suggested in the mailing list is that low mobility for PMIP6 is applicable only in those access networks wherein the access network elements are aware of the state of the MN's connection and congestion state. The MAG can use this information to signal to an

LMA attachment state and potentially cause flows to be switched to an alternative MAG. It may be okay to have specific statements about the limitations of flow mobility for PMIPv6 documented as a sort of disclaimer.

This document aims to make clear about what is in scope of this work and some of the limitations as well.

## 5. IANA Considerations

This document makes no request of IANA.

## 6. References

### 6.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC RFC 5213, August 2008.

### 6.2. Informative References

- [I-D.ietf-netext-logical-interface-support]  
Melia, T. and S. Gundavelli, "Logical Interface Support for multi-mode IP Hosts",  
draft-ietf-netext-logical-interface-support-03 (work in progress), September 2011.
- [I-D.ietf-netext-pmipv6-flowmob-ob]  
Bernardos, CJ., "Proxy Mobile IPv6 Extensions to Support Flow Mobility", draft-ietf-netext-pmipv6-flowmob-01 (work in progress), September 2011.
- [I-D.koodli-netext-multiaccess-indicator]  
Koodli, Rajeev. and Jouni. Korhonen, "Multi-access Indicator for Mobility",  
draft-koodli-netext-multiaccess-indicator-02 (work in progress), August 2011.
- [RFC5677] Melia, T., Bajko, G., Das, S., Golmie, N., and JC. Zuniga, "IEEE 802.21 Mobility Services Framework Design (MSFD)", RFC RFC 5677, December 2009.

[TS23261] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP flow mobility and seamless Wireless Local Area Network (WLAN) offload;", 3GPP 3GPP TS 23.261, September 2010.

## Authors' Addresses

Tian Tian  
ZTE  
No.68 Zijinghua Rd  
Nanjing, Yuhuatai District 210012  
China.P.R

Phone: +86-25-5287-1267  
Email: tian.tian1@zte.com.cn

Wei Yan  
ZTE  
No.68 Zijinghua Rd  
Nanjing, Yuhuatai District 210012  
China.P.R

Phone: +86-25-5287-0503  
Email: yan.wei8@zte.com.cn

Yuan Wei  
ZTE  
No.68 Zijinghua Rd  
Nanjing, Yuhuatai District 210012  
China.P.R

Phone: +86-25-5287-1091  
Email: wei.yuan2@zte.com.cn



netext  
Internet-Draft  
Intended status: Standards Track  
Expires: April 15, 2012

Y. Tu  
C. Zhu  
ZTE  
October 13, 2011

MN Status Option for Proxy Mobile IPv6  
draft-tu-netext-mn-status-option-00

Abstract

This document explains how the LMA obtains the MN status in order to decide and perform the flow mobility.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on April 15, 2012.

Copyright Notice

Copyright (c) 2011 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	3
2. Conventions used in this document . . . . .	3
3. MN status option for PMIPv6 . . . . .	3
3.1. Overview . . . . .	3
3.2. Mobile Node Status Option . . . . .	4
4. Security Considerations . . . . .	5
5. IANA Considerations . . . . .	5
6. Contributors . . . . .	5
7. Normative References . . . . .	5
Authors' Addresses . . . . .	5

## 1. Introduction

There is a need for the local mobility anchor to decide and perform the flow mobility from one access network to another, e.g. from 3GPP to WLAN or from WLAN to WiMAX. Proxy Mobile IPv6 specification [RFC5213] allows carrying of the Access Technology Type information from the mobile access gateway to the local mobility anchor. However, the Access Technology Type information is insufficient to provide the local mobility anchor enough information to guarantee the flow mobility is successfully completed, in which the mobile node status (e.g. connect, disconnect or idle/power saving mode) is unknown for the local mobility anchor. In this case, the local mobility anchor may choose one of the access networks which is currently unavailable as the target to move a specific IP flow according to the operator preferences and local policies. To prevent this, the mobile node status needs to be updated from the mobility access gateway to the local mobility anchor.

This document defines a new mobility option, MN Status option for Proxy Mobile IPv6 (PMIPv6), that can be used by mobile access gateway (MAG) for carrying the MN status with the correspondent access network to the local mobility anchor.

## 2. Conventions used in this document

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].

## 3. MN status option for PMIPv6

### 3.1. Overview

In some deployments the network (e.g. 3GPP) needs to support the multiple access technologies for the mobile node, and the local mobility anchor can be triggered to decide which access technology will be used to move the particular IP flow according to the operator preferences and local policy. To guarantee the flow mobility procedure from one access technology to another is successful, one of the key information should be obtained by the LMA is the currently mobile node status with correspondent access network type information.

The mobility access gateway is the right one to detect the mobile node status using the mechanisms as defined in RFC5213, furthermore, each access network has defined its own mechanisms to detect the

connectivity status of the attached mobile node.

The mobile node status can be carried in the messages exchange between the MAG and LMA, be more specific, the MAG can periodic or be event triggered to update the MN status to the LMA. How the LMA use this information is outside the scope of this document.

### 3.2. Mobile Node Status Option

A new option, Mobile Node Status Option, is defined for using it in messages (e.g. PBU and PBA) exchanged between a local mobility anchor and a mobile access gateway.

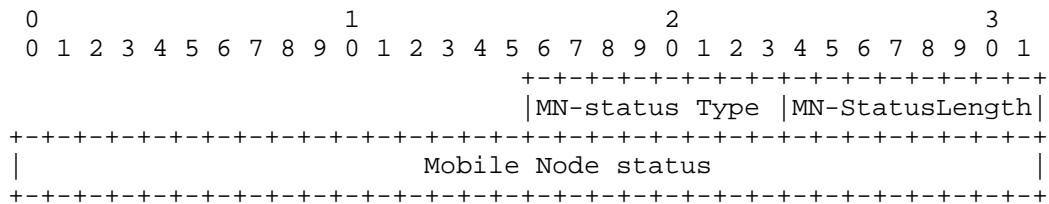


Figure 1: MN Status Option

MN-status Type

TBD

MN-status Length

8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields.

Mobile Node status

The status of the mobile node attached from a specific access network, such as WiFi, WiMAX and 3GPP. Currently the value of the MN status can be as follow:

1, connect mode,

2, disconnect mode,

3, idle/Power saving mode



4,reserved.

#### 4. Security Considerations

TBD

#### 5. IANA Considerations

TBD

#### 6. Contributors

The following people contributed to this document (in no specific order):

Yifeng Bi  
ZTE  
bi.yifeng@zte.com.cn

#### 7. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 2011.

#### Authors' Addresses

Yangwei Tu  
ZTE  
Nanjing  
Nanjing  
China  
  
Email: tu.yangwei@zte.com.cn

Chunhui Zhu  
ZTE  
Nanjing  
Nanjing  
China

Email: zhu.chunhui@zte.com.cn

