

NETEXT WG  
Internet-Draft  
Intended status: Informational  
Expires: April 21, 2014

T. Melia, Ed.  
Alcatel-Lucent  
S. Gundavelli, Ed.  
Cisco  
October 18, 2013

Logical Interface Support for multi-mode IP Hosts  
draft-ietf-netext-logical-interface-support-08

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 operating in 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 context 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 April 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 . . . . .	3
2. Terminology . . . . .	4
3. Hiding Link-layer Technologies - Approaches and Applicability . . . . .	5
3.1. Link-layer Abstraction - Approaches . . . . .	5
3.2. Applicability Statement . . . . .	6
3.2.1. Link layer support . . . . .	6
3.2.2. Logical Interface . . . . .	6
4. Technology Use cases . . . . .	8
5. Logical Interface Functional Details . . . . .	9
5.1. Configuration of a Logical Interface . . . . .	10
5.2. Logical Interface Forwarding Conceptual Data Structures . . . . .	10
6. Logical Interface Use-cases in Proxy Mobile IPv6 . . . . .	12
6.1. Multihoming Support . . . . .	12
6.2. Inter-Technology Handoff Support . . . . .	13
6.3. Flow Mobility Support . . . . .	14
7. IANA Considerations . . . . .	15
8. Security Considerations . . . . .	16
9. Authors . . . . .	17
10. Acknowledgements . . . . .	17
11. References . . . . .	18
11.1. Normative References . . . . .	18
11.2. Informative References . . . . .	18
Authors' Addresses . . . . .	19

## 1. Introduction

Proxy Mobile IPv6 [RFC5213] is a network-based mobility protocol. Some of the key goals of the protocol include support for multihoming, inter-technology handoffs and flow mobility support. The base protocol features specified in [RFC5213] and [RFC5844] allow the mobile node to attach to the network using multiple interfaces (simultaneously or sequentially), or to perform handoff between different interfaces of the mobile node. However, for supporting these features, the mobile node is required to be activated with specific software configuration that allows the mobile node to either perform inter-technology handoffs between different interfaces, attach to the network using multiple interfaces, or perform flow movement from one access technology to another. This document analyzes from the mobile node's perspective a specific approach that allows the mobile node to leverage these mobility features. Specifically, it explores the use of the Logical Interface support, a semantic available on most operating systems.

A Logical Interface is a construct internal to the operating system. It is an approach where a logical link-layer implementation hides a variety of physical interfaces from the IP stack. This semantic has been used on a variety of operating systems to implement applications such as Mobile IP clients [RFC6275] and IPsec VPN clients [RFC4301].

In the context of an access infrastructure providing network network-based mobility management services across a variety of access technologies, as provided by a Proxy Mobile IPv6 domain [RFC5213], a logical interface can be used to afford inter-technology handover, multihoming, and/or flow mobility without requiring from the mobile node IP stack specific support to that effect.

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 logical interface and network elements in the Proxy Mobile IPv6 domain when supporting the aforementioned mobility management features. It also analyzes the issues involved with this approach 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 introduces the following terms:

PIF (Physical Interface) - a network interface card attached to an an host providing network connectivity (e.g. an Ethernet card, a WLAN card, an LTE interface).

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

Sub-If (Sub Interface) - a physical 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/mechanisms that allow hiding access technology changes or movement from host IP layer. 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 in a Proxy Mobile IPv6 domain [RFC5213].

#### 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 that logically group/bond 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.

### 3.2. Applicability Statement

We now focus on the applicability of the above solutions against the following requirements:

- o multi technology support
- o sequential vs. simultaneous access

#### 3.2.1. 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.

#### 3.2.2. 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.

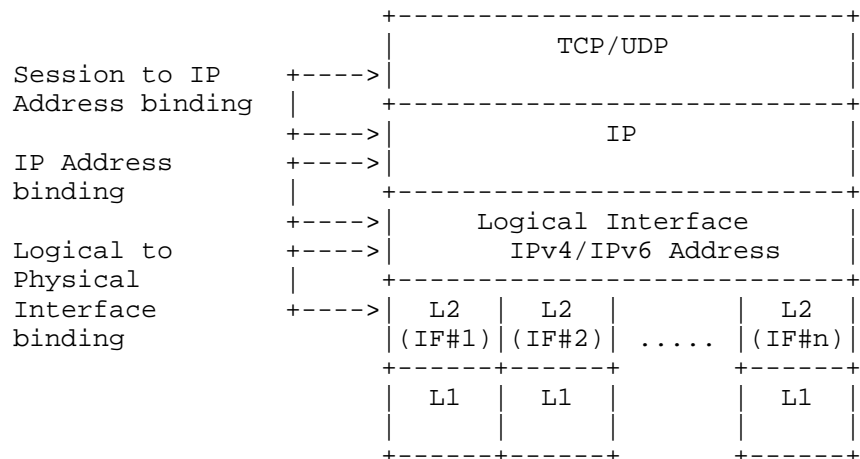


Figure 1: General overview of logical interface

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 Conceptual Data Structures

The logical interface maintains the list of sub-interfaces that are part of the logical interface. This conceptual data structure is called as the LIF 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 RoutingPolicies	FLOW ID	Physical_Intf_Id
	Link Status		
PIF_ID	FLOW RoutingPolicies	FLOW_ID	Physical_Intf_Id
	Link Status		
....	....	....	....

Figure 2

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.

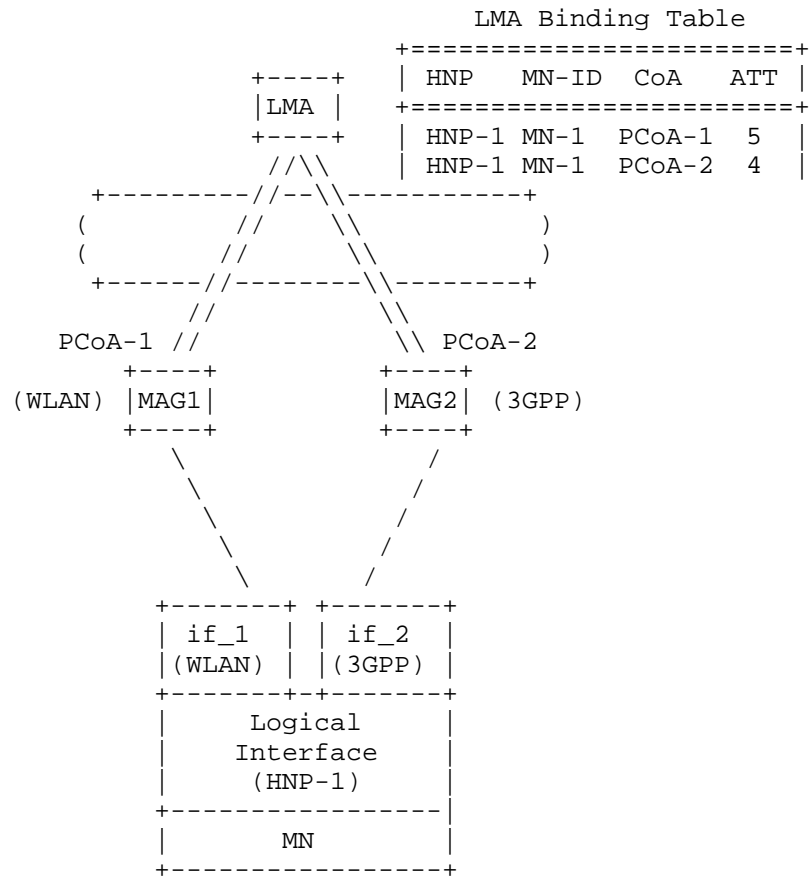


Figure 3: Multihoming Support

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.

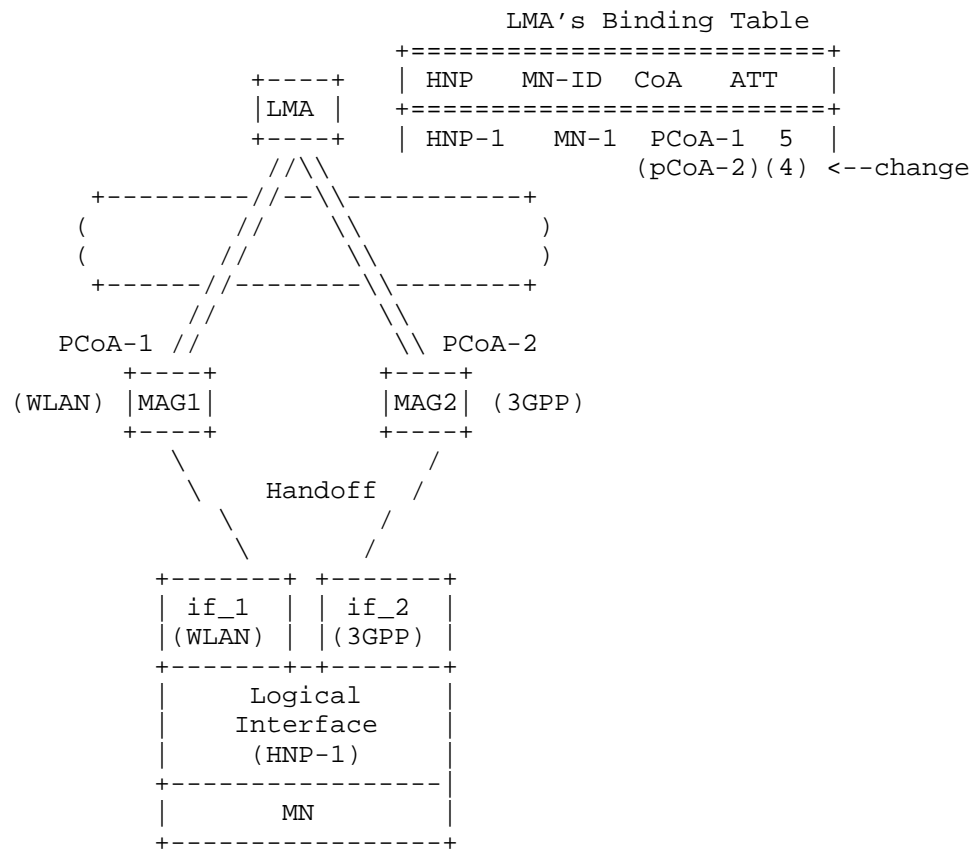


Figure 4: Inter-Technology Handoff Support

- 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 flow mobility support, 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.

## 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.



## 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

Julien Laganier

jlaganier@JUNIPER.NET

## 10. Acknowledgements

The authors would like to acknowledge prior 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, and Julien Laganier for all the discussions on this topic.

## 11. References

## 11.1. Normative References

- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 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.

## 11.2. Informative References

- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- [RFC5072] Varada, S., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.
- [RFC5677] Melia, T., Bajko, G., Das, S., Golmie, N., and JC. Zuniga, "IEEE 802.21 Mobility Services Framework Design (MSFD)", RFC 5677, December 2009.
- [RFC6085] Gundavelli, S., Townsley, M., Troan, O., and W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", RFC 6085, January 2011.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6418] Blanchet, M. and P. Seite, "Multiple Interfaces and Provisioning Domains Problem Statement", RFC 6418, November 2011.
- [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)  
Alcatel-Lucent  
Route de Villejust  
Nozay 91620  
France

Email: telemaco.melia@alcatel-lucent.com

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

Email: sgundave@cisco.com



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.

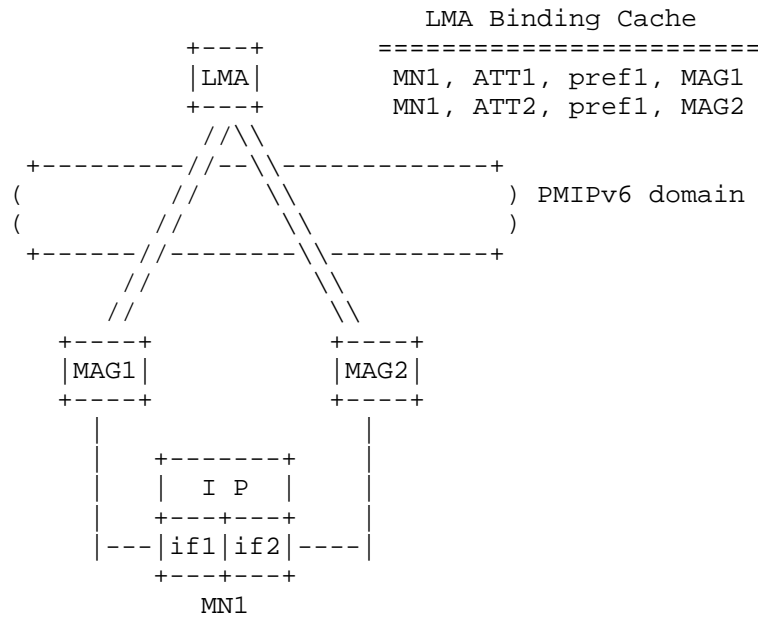


Figure 1: Shared prefix across physical interfaces scenario

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.

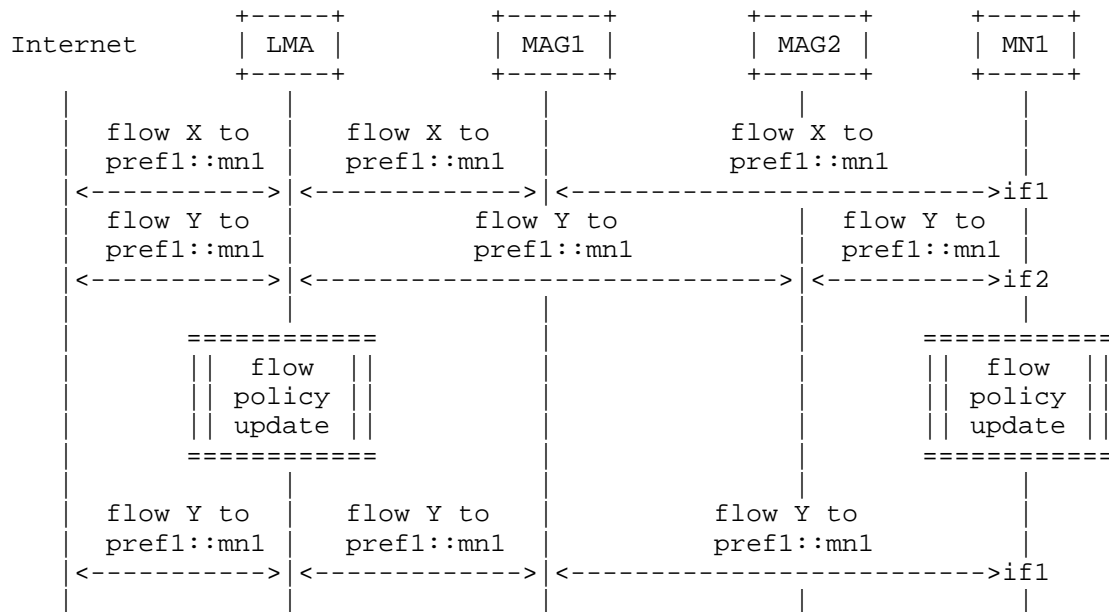


Figure 2: Flow mobility message sequence with common set of prefixes

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.

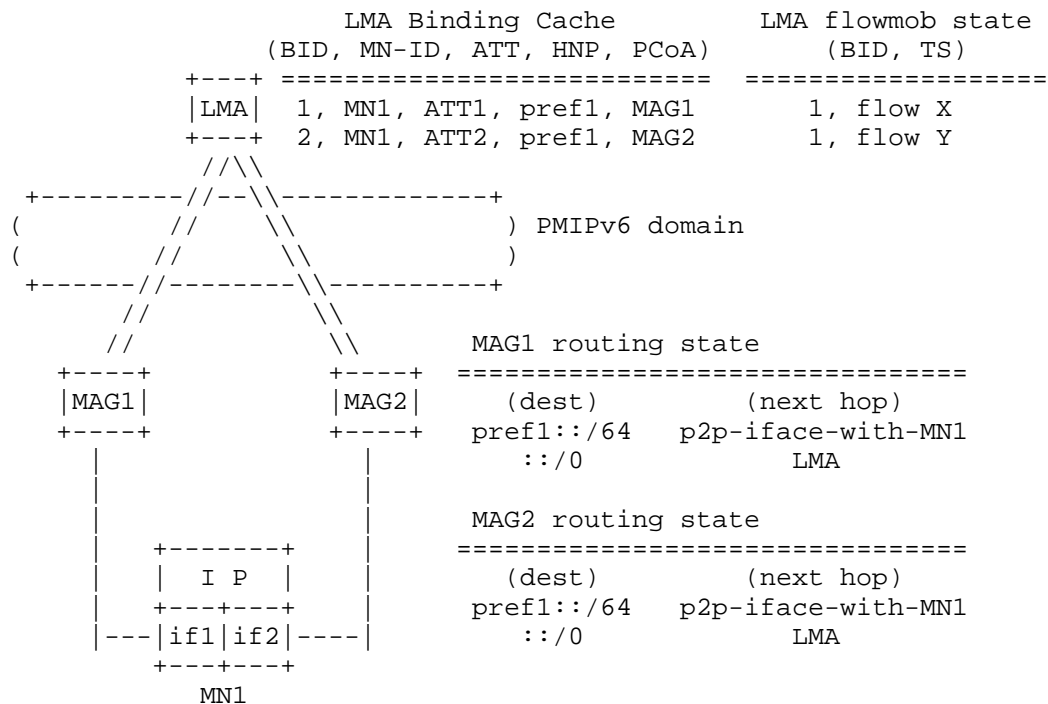


Figure 3: Data structures with common set of prefixes

### 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.

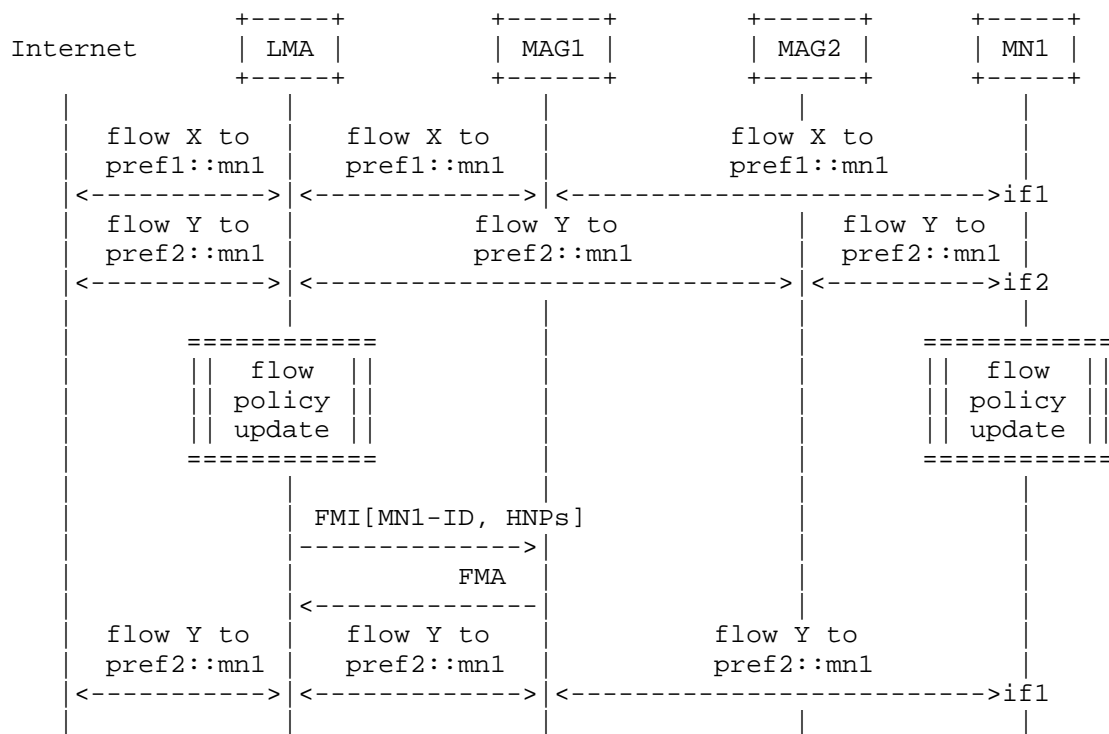


Figure 4: Flow mobility message sequence when the LMA assigns different sets of prefixes per physical interface

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.

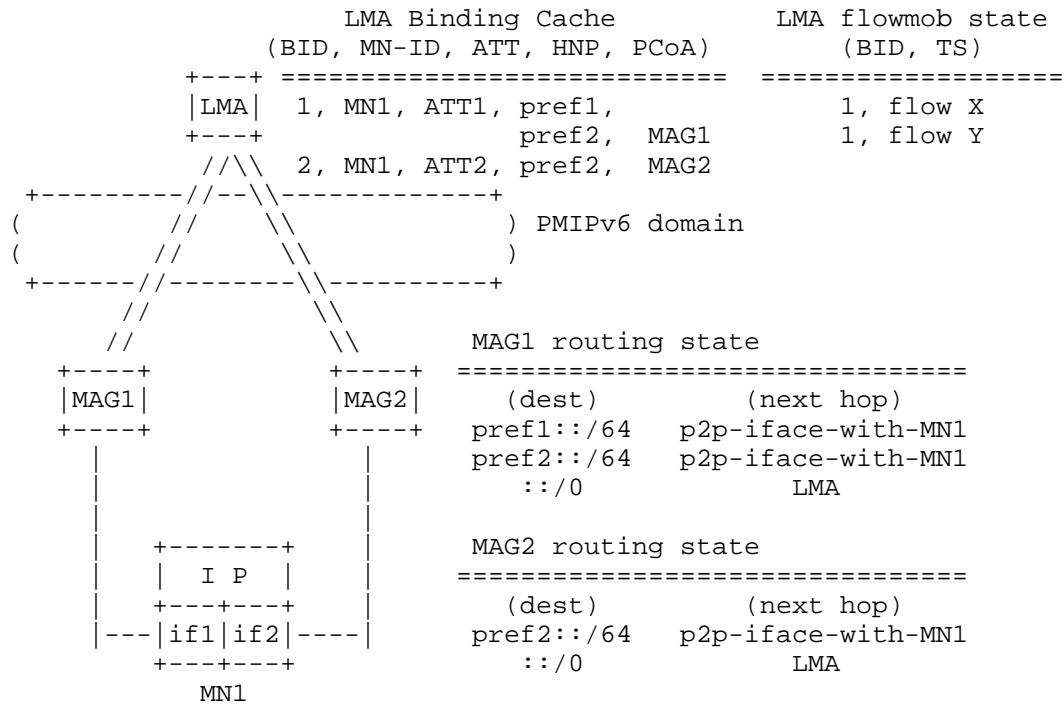


Figure 5: Data structures when the LMA assigns a different set of prefixes

### 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.

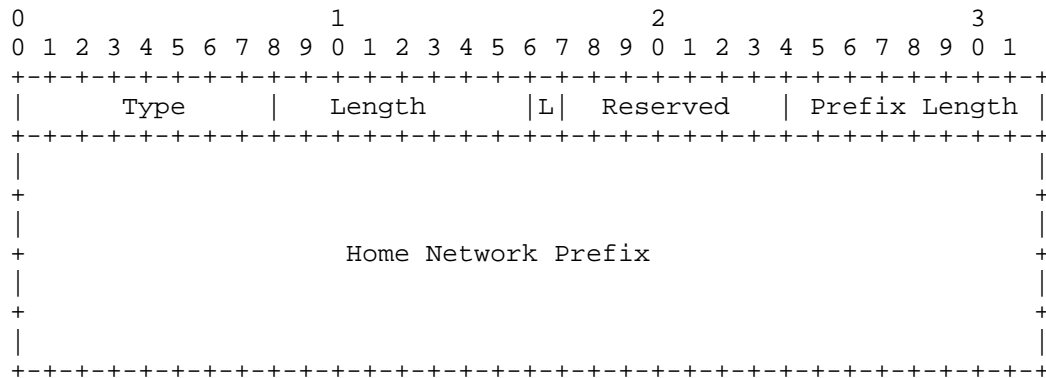
This specification requires implementation of UPN [RFC7077] and UPA [RFC7077] messages with the specific Notification Reason and Status Code values as defined by this document. This document does not require implementation of any other aspects of [RFC7077].

### 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/>

INTERNET-DRAFT  
Intended Status: Informational  
Expires: August 14, 2014

John Kaippallimalil  
Huawei  
Rajesh S. Pazhyannur  
Cisco  
Parviz Yegani  
Juniper  
February 10, 2014

Mapping 802.11 QoS in a PMIPv6 Mobility Domain  
draft-kaippallimalil-netext-pmip-qos-wifi-04

Abstract

This document provides recommendations on procedures and mapping of QoS parameters between 802.11 and PMIPv6. QoS parameters in 802.11 that reserve resources for 802.11 streams should be mapped to PMIPv6 QoS resources for IP sessions and flows. QoS reservation sequences in 802.11 should allow cases where MN initiate resource reservation, as well as cases where the network initiates resource reservation. Additionally, it should be possible for QoS parameters for PMIPv6 flows and mobility sessions to be mapped to 802.11 traffic stream reservations. The sequences and parameters to be mapped to provide a consistent behavior across 802.11 and PMIPv6 QoS are described here.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

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

The list of Internet-Draft Shadow Directories can be accessed at



<http://www.ietf.org/shadow.html>

#### Copyright and License Notice

Copyright (c) 2014 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
1.1. Terminology . . . . .	4
1.2. Definitions . . . . .	5
1.3. Abbreviations . . . . .	6
2. End-to-End QoS with no Admission Control . . . . .	6
3. End-to-End QoS with Admission Control . . . . .	8
3.1. Case A: MN Initiates QoS Request . . . . .	9
3.2. Case B: Network Initiates QoS Signaling (802.11aa based) . . . . .	11
3.3. Case C: Hybrid (Network Initiated for PMIP, MN initiated in 802.11) . . . . .	12
3.4. Case D: Network Initiated Release . . . . .	14
3.5. Case E: MN Initiated Release . . . . .	16
3.6. Service Guarantees in 802.11 . . . . .	17
4. Mapping of QoS Parameters . . . . .	17
4.1 Connection Mapping . . . . .	18
4.2. QoS Class . . . . .	18
4.3. Bandwidth . . . . .	19
4.4. Preemption Priority . . . . .	20
5. Security Considerations . . . . .	20
6. IANA Considerations . . . . .	21
7. References . . . . .	21
7.1. Normative References . . . . .	21
7.2. Informative References . . . . .	21
Authors' Addresses . . . . .	22
Appendix A: QoS in 802.11, PMIPv6 and 3GPP Networks . . . . .	23
A.1. QoS in IEEE 802.11 Networks . . . . .	23

A.2. QoS in PMIPv6 Mobility domain . . . . .	23
A.3. QoS in 3GPP Networks . . . . .	24

## 1. Introduction

802.11 networks can currently apply QoS policy by using ALG (Application Level Gateway) to detect an application (e.g. SIP signaling) and then install QoS for the corresponding IP flow on the Wireless LAN Controller (WLC)/ Access Point (AP). However, this is not a general mechanism and would require ALG or detection of application level semantics in the access to install the right QoS.

[PMIP-QoS] describes a application neutral procedure to obtain QoS for PMIPv6 flows and sessions. However, there are differences in parameters and procedures that need to be mapped between PMIPv6 QoS and 802.11. PMIPv6 has the notion of QoS for mobility sessions and flows while in 802.11 these should correspond to QoS for 802.11 data frames. Parameters in 802.11 QoS do not always have a one-to-one correspondence in PMIPv6 QoS. Further, 802.11 and PMIP QoS procedures need to be aligned based on whether QoS setup is triggered by the MN or pushed by the the network, as well as working with WMM or 802.11aa mechanisms.

This document provides information on using PMIPv6 QoS parameters for an MN connection over a 802.11 access network. The recommendations here allow for dynamic QoS policy information per Mobile Node (MN) and session to be configured by the 802.11 access network. PMIPv6 QoS signaling between MAG and LMA provisions the per MN QoS policies in the MAG. In the 802.11 access network modeled here, the MAG is located at the Access Point (AP)/ Wireless LAN Controller (WLC) . Figure 1 below provides an overview of the entities and protocols.

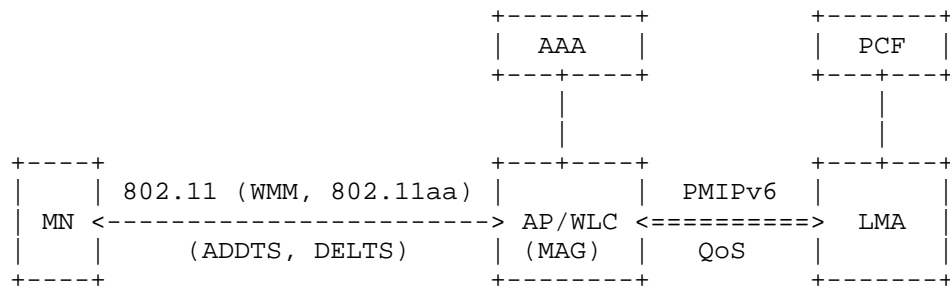


Figure 1: QoS Policy in 802.11 Access

MN and AP/WLC use 802.11 QoS mechanisms to setup admission controlled

flows. The AP/WLC is a MAG that requests for QoS policy from the LMA. The MN uses ADDTS (Add Traffic Stream) to setup QoS for a traffic stream between itself and the AP, and DELTS (Delete Traffic Stream) to delete that stream. In WMM [WMM 1.2.0], the AP advertises if admission control is mandatory for an access class. Admission control for best effort or background access classes is not recommended. In addition to WMM capability, 802.11aa allows for AP/WLC to support an ADDTS reservation request to the MN. This makes it simpler to support a PMIPv6 QoS request that is pushed to the AP/WLC.

The parameter mapping recommendations described here support the procedures by which the 3GPP network provisions QoS per application dynamically or during authorization of the Mobile Node (MN). However, the 802.11 procedures described here are not limited to work for just the 3GPP policy provisioning. If PMIPv6 QoS parameters can be provisioned on the MAG via mechanisms defined in [PMIP-QoS], the 802.11 procedures can be applied in general for provisioning QoS in a 802.11 network.

PMIPv6 QoS parameters need to be mapped to 802.11 QoS parameters. In some cases, there is no one-to-one mapping. And in other cases such as bandwidth, the values received in PMIP should be mapped to the right 802.11 parameters. This document provides recommendations to perform QoS mapping between PMIPv6 and 802.11 QoS.

[PMIP-QoS] does not explicitly describe how the QoS signaling and QoS sub-options map into corresponding signaling and parameters in the 802.11 access network. This mapping and the procedures in the 802.11 network to setup procedures are the focus of this document. The end-to-end flow spanning 802.11 access and PMIPv6 domain and the QoS parameters in both segments are described here. Thus, it provides a systematic way to map the various QoS parameters available in initial authorization, as well as setup of new sessions (such as a voice/video call). The mapping recommendations allow for proper provisioning and consistent interpretation between the various QoS parameters provided by PMIP QoS, and 802.11.

The rest of the document is organized as follows. Chapter 2 provides an overview of establishing mobility sessions with no admission control. These mechanisms are specified in [PMIP QoS] and outlined here since the mobility session established is the basis for subsequent admission controlled requests for flows. Chapter 3 describes how end to end QoS with 802.11 admission control is achieved. The mapping of parameters between 802.11 and PMIP QoS is described in Chapter 5.

### 1.1. 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 RFC 2119 [RFC2119].

## 1.2. Definitions

### Guaranteed Bit Rate (GBR)

GBR in a mobile network defines the guaranteed (reserved) bit rate resources of service data flow on a connection (bearer) [TS23.203].

### Maximum Bit Rate (AMBR)

MBR represents the maximum bandwidth of a flow with reservation.

### Aggregate Maximum Bit Rate (MBR)

AMBR represents the total bandwidth that all flows of a user is allowed. AMBR does not include flows with reservation.

### Allocation Retention Priority (ARP)

ARP is used in the mobile network to determine the order in which resources for a flow may be preempted during severe congestion or other resource limitation. ARP of 1 is the highest priority while 15 is the lowest [TS23.203].

### Peak Data Rate

In WMM, Peak Data Rate specifies the maximum data rate in bits per second. The Maximum Data Rate does not include the MAC and PHY overheads [WMM 1.2.0].

### Mean Data Rate

This is the average data rate in bits per second. The Mean Data Rate does not include the MAC and PHY overheads [WMM1.2.0]

### Minimum Data Rate

In WMM, Minimum Data Rate specifies the minimum data rate in bits per second. The Minimum Data Rate does not include the MAC and PHY overheads [WMM 1.2.0].

### TSPEC

The TSPEC element in 802.11 contains the set of parameters that define the characteristics and QoS expectations of a traffic flow.

### TCLAS

The TCLAS element specifies an element that contains a set of parameters necessary to identify incoming MSDU (MAC Service Data Unit) that belong to a particular TS (Traffic Stream) [802.11].

### 1.3. Abbreviations

3GPP	Third Generation Partnership Project
AAA	Authentication Authorization Accounting
AMBR	Aggregate Maximum Bit Rate
ARP	Allocation and Retention Priority
AP	Access Point
DSCP	Differentiated Services Code Point
EPC	Enhanced Packet Core
GBR	Guaranteed Bit Rate
MAG	Mobility Access Gateway
MBR	Maximum Bit Rate
MN	Mobile Node
PCF	Policy Control Function
PDN-GW	Packet Data Network Gateway
QCI	QoS Class Indicator
QoS	Quality of Service
TCLAS	Type Classification
TSPEC	Traffic Conditioning Spec
WLC	Wireless Controller

## 2. End-to-End QoS with no Admission Control

PMIPv6 and 802.11 QoS with no admission control is specified in [PMIP QoS]. This section is provided as background here since prior to the establishment of an admission controlled flow, a mobility session as described here is established. IETF (RFC 4594) and GSMA have defined mapping between DSCP and IEEE 802.11 UP (User Priority). The AP/WLC (MAG) should be pre-configured to use the mapping from one of these specifications.

An MN that attempts to connect to a 802.11 network typically authenticates first and may have an authorization profile downloaded. The AP/WLC may use the QoS profile for the MN for policing flows. However, the network can obtain more dynamic policy that corresponds to current mobile network conditions and preferences using PMIP QoS.

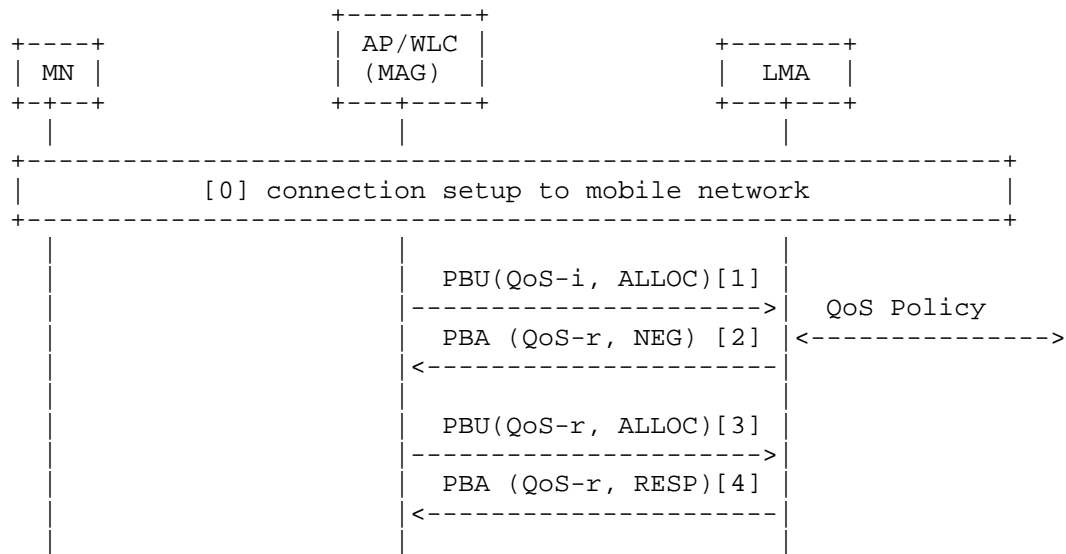


Figure 2: Default connection setup

- [0] MN signals to setup connection. The AP/WLC obtains an authorization profile that includes QoS information, or may have an administratively configured profile with QoS information.
- [1] The completion of 802.11 and IP setup serves as a trigger for the MAG (AP/WLC) to request for dynamic QoS parameters. The MAG sends a PBU containing QoS Option with operation code set to ALLOCATE, and DSCP, QoS Attributes set to initially authorized values for the MN's default connection (QoS-i).

This request is for QoS of all flows of a connectivity session of the MN and includes DSCP, Per-MN-Agg-Max-DL-Bit-Rate, Per-MN-Agg-Max-UL-Bit-Rate, Per-Session-Agg-Max-DL-Bit-Rate, Per-Session-Agg-Max-UL-Bit-Rate and Allocation-Retention-Priority fields derived from the MN initial authorization profile. The Traffic Selector field should not be present.

- [2] The LMA queries the policy server and obtains a response. The policy server may grant the QoS requested or may change the QoS levels based on network or other dynamic conditions (QoS-r in figure). This example assumes that the LMA cannot provide the QoS requested by the MAG.

The LMA sets the operational code to NEGOTIATE and responds with downgraded parameters for DSCP, Per-MN-Agg-Max-DL-Bit-Rate, Per-MN-Agg-Max-UL-Bit-Rate, Per-Session-Agg-Max-DL-Bit-Rate, Per-

Session-Agg-Max-UL-Bit-Rate and Allocation-Retention-Priority. The Traffic Selector field is not present since the provisioning applies to the entire PMIPv6 connectivity session.

[3] The MAG receives the downgraded QoS and sends a revised PBU with the QoS options that the LMA is prepared to offer. The operational code is set to ALLOCATE.

[4] The LMA can accept the requested QoS. The LMA sends a PBA message with the revised QoS options and operational code set to RESPONSE.

The new QoS values will be used by the MAG to police flows of the MN and will supercede earlier (or initially) provisioned QoS values. MAG polices session flows to not exceed Per-Session-Agg-Max-DL-Bit-Rate, Per-Session-Agg-Max-UL-Bit-Rate. If there are multiple sessions, the total bandwidth should not exceed Per-MN-Agg-Max-DL-Bit-Rate, Per-MN-Agg-Max-UL-Bit-Rate.

### 3. End-to-End QoS with Admission Control

This section outlines a few use cases to illustrate how parameters and mapping are applied for flows that require admission control. These cases illustrate the various provisioning sequences and mechanisms. It is not intended to be exhaustive.

The general procedure here is that a flow that requires admission control is part of a PMIPv6 connectivity session. QoS options for the overall session are provisioned as described in section 2. As a result of some application layer signaling, specific flows of the application may require admission controlled QoS which can be provisioned on a per flow basis.

There are two main types of interaction possible to provision QoS for flows that require admission control - one case is where the MN initiates the QoS request and the network provisions the resources. The second is where the network provisions resources as a result of some out of band signaling (like application signaling). In the second scenario, if the MN supports 802.11aa, the network can push the QoS configuration to the MN. If the MN only supports WMM QoS, then MN requests for QoS for the 802.11 segment and the MAG provisions based on QoS already provisioned for the MN. These three cases are described in sections 3.1 - 3.3.

In each of the sequences, QoS parameters need to be mapped between 802.11 and PMIPv6. The table below provides an overview of the mapping for establishing QoS for an admission controlled flow.

Further details of the parameters and mappings are provided in section 4.

MN <--> AP/WLC(802.11)	AP/WLC(MAG) <--> LMA PMIPv6
(TCLAS) TCP/UDP IP	Traffic Selector (IP flow)
(TCLAS) User Priority	DSCP
(TSPEC)Minimum Data Rate, DL	Guaranteed-DL-Bit-Rate
(TSPEC)Minimum Data Rate, UL	Guaranteed-UL-Bit-Rate
(TSPEC)Mean Data Rate UL/DL	-
(TSPEC)Peak Data Rate, DL	Aggregate-Max-DL-Bit-Rate
(TSPEC)Peak Data Rate, UL	Aggregate-Max-UL-Bit-Rate

Table 1: 802.11 - PMIPv6 QoS Parameter Mapping

### 3.1. Case A: MN Initiates QoS Request

During an MN flow setup that requires admission control in the 802.11 network, QoS parameters for the flow needs to be provisioned. This procedure outlines the case where the MN is configured (e.g. in SIM) to start the QoS signaling. In this case, the MN sends an ADDTS request indicating the QoS required for the flow. The AP/WLC (MAG) obtains the corresponding level of QoS to be granted to the flow by PMIPv6 PBU/PBA sequence with QoS options with the LMA. Details of the QoS provisioning for the flow are described below.



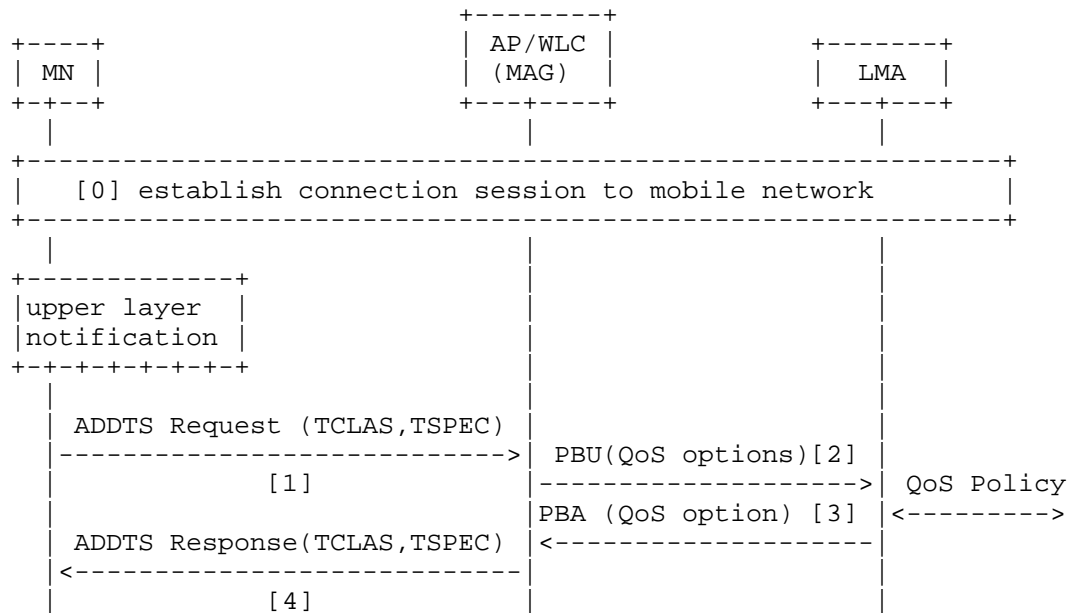


Figure 3: MN initiated QoS setup

[0] The MN has a best effort connectivity session as described in section 2. This allows the MN to perform application level signaling and setup.

[1] The trigger for MN to request QoS is an upper layer notification. This may be the result of end-to-end application signaling and setup procedures (e.g. SIP)

If the MN is configured to start QoS signaling, the MN sends an ADDTS request with TSPEC and TCLAS identifying the flow for which QoS is requested. The TSPECs for both uplink and downlink in this request should contain the Minimum Data Rate and Peak Data Rate .

[2] If there are sufficient resources at the AP/WLC to satisfy the request, the MAG (AP/WLC) sends a PBU with QoS options, operational code ALLOCATE and Traffic Selector identifying the flow. The Traffic selector is derived from the TCLAS to identify the flow requesting QoS. 802.11 QoS parameters in TSPEC are mapped to PMIPv6 parameters. The mapping of TCLAS and TSPEC parameters to PMIPv6 is shown in Table 1.

[3] The LMA obtains the authorized QoS for the flow and responds to the MAG with operational code set to RESPONSE. Mapping of PMIPv6

parameters to 802.11 TSPEC and TCLAS is shown in Table 1.

In networks like 3GPP, the reserved bandwidth for flows are accounted separately from the non-reserved session bandwidth. The Traffic Selector identifies the flow for which the QoS reservations are made.

- [4] The AP/WLC (MAG) provisions the corresponding QoS and replies with ADDTS Response containing authorized QoS in TSPEC and flow identification in TSPEC.

The AP/WLC polices these flows according to the QoS provisioning.

### 3.2. Case B: Network Initiates QoS Signaling (802.11aa based)

In some cases (e.g. LTE/SAE), the policy server in the network may be configured to initiate the policy reservation request for a flow. This use case illustrates how an MN and 802.11 network that support 802.11aa can provision QoS to flows of the MN that when the policy server pushes the reservation request.

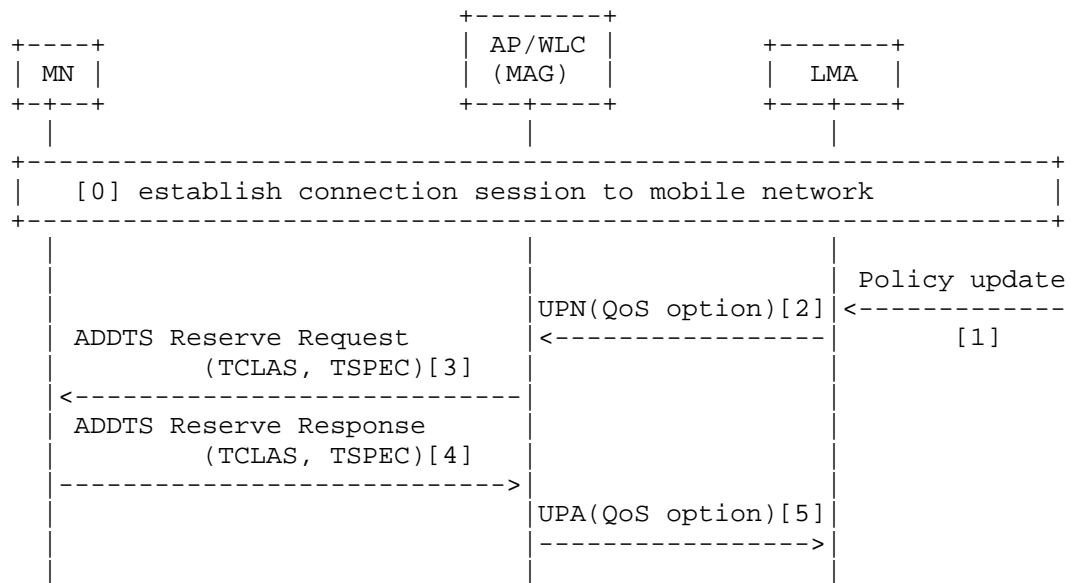


Figure 4: Network initiated QoS setup with 802.11aa

- [0] The MN sets up best effort connectivity session as described in Case A. This allows the MN to perform application level

signaling and setup.

- [1] The policy server sends a QoS reservation request to the LMA. This is usually sent in response to an application that requests the policy server for higher QoS for some of its flows.

The LMA reserves resources for the flow requested.

- [2] LMA sends PMIP UPN (Update Notification) to the MAG with QoS parameters for the flow for which the LMA reserved resources in step [1]. In UPN, the operational code in QoS option is set to ALLOCATE and the Traffic Selector identifies the flow for QoS.

The LMA QoS parameters include Guaranteed-DL-Bit-Rate/Guaranteed-UL-Bit-Rate and Aggregate-Max-DL-Bit-Rate/Aggregate-Max-UL-Bit-Rate for the flow. In networks like 3GPP, the reserved bandwidth for flows are accounted separately from the non-reserved session bandwidth.

- [3] If there are sufficient resources to satisfy the request, the AP/WLC (MAG) sends an ADDTS Reserve Request (802.11aa) specifying the QoS reserved for the traffic stream including TSPEC and TCLAS element mapped from PMIP QoS Traffic Selector to identify the flow.

PMIPv6 parameters are mapped to TCLAS and TSPEC as shown in Table 1.

If there are insufficient resources at the AP/WLC, the MAG will not send an ADDTS message and will continue processing of step [5].

- [4] MN accepts the QoS reserved in the network and replies with ADDTS Reserve Response.
- [5] The MAG (AP/WLC) replies with UPA confirming the acceptance of QoS options and operational code set to RESPONSE. The AP/WLC police flows based on the new QoS.

If there are insufficient resources at the AP/WLC, the MAG sends a response with UPA status code set to CANNOT\_MEET\_QOS\_SERVICE\_REQUEST.

### 3.3. Case C: Hybrid (Network Initiated for PMIP, MN initiated in 802.11)

This use case outlines a scenario where an MN attaches to the 802.11

and then obtains services in the mobile network. When the MN attaches, PMIP signaling between the MAG and LMA establishes mobile connection and related QoS. Subsequently, the MN starts an application that requires dedicated bandwidth resources and signals that using TSPEC/ADDTS request. The details of this sequence are described below.

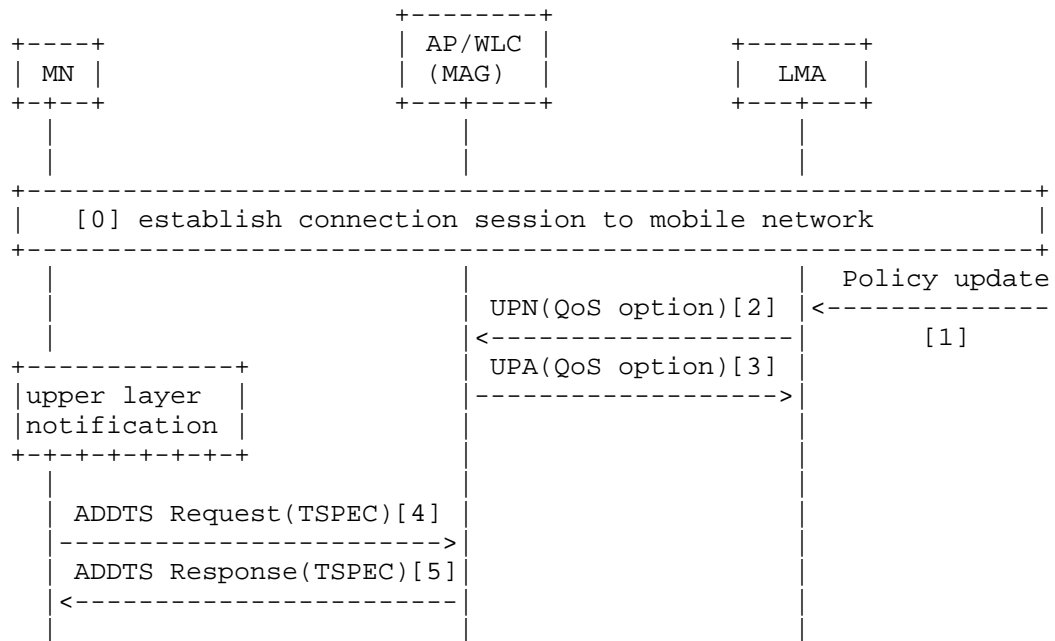


Figure 5: Network initiated QoS setup with WMM

- [0] The MN sets up best effort connectivity session as described in Case A. This allows the MN to perform application level signaling and setup.
- [1] The policy server sends a QoS reservation request to the LMA. This is usually sent in response to an application that requests the policy server for higher QoS for some of its flows.

The LMA reserves resources for the flow requested.

- [2] LMA sends PMIP UPN (Update Notification) to the MAG with QoS option operational code set to ALLOCATE and QoS parameters for which the LMA reserved resources in step [1]. In UPN, the Traffic selector field in QoS Option identifies the flow for QoS.

The LMA QoS parameters include Guaranteed-DL-Bit-

Rate/Guaranteed-UL-Bit-Rate and Aggregate-Max-DL-Bit-Rate/Aggregate-Max-UL-Bit-Rate for the flow. In networks like 3GPP, the reserved bandwidth for flows are accounted separately from the non-reserved session bandwidth. This is indicated by using the Traffic Selector in PMIPv6 QoS.

- [3] If there are sufficient resources to satisfy the request, the MAG (AP/WLC) replies with UPA confirming the acceptance of QoS options and operation code set to RESPONSE. If there are insufficient resources at the AP/WLC, the MAG may send a response with UPA status code set to CANNOT\_MEET\_QOS\_SERVICE\_REQUEST.

The AP/WLC can police flows based on the new QoS. However, the AP/WLC does not initiate QoS reservation signaling on 802.11 because either it or the MN does not support 802.11aa.

- [4] The trigger for the MN to request QoS is an upper layer notification. This may be the result of end-to-end application signaling and setup procedures (e.g. SIP)

The MN sends an ADDTS request with TSPEC and TCLAS identifying the flow for which QoS is requested. The TSPECs for both uplink and downlink in this request should contain the Minimum Data Rate and Peak Data Rate. The MAG maps PMIPv6 parameters obtained earlier as shown in Table 1.

If the MN supports only WMM QoS, TCLAS is not sent. The AP/WLC may identify the flow based on connection signaling (e.g. 3GPP 23.402, WCS), most recent updates from PMIP QoS (i.e. that in message [3] above), or some combination thereof.

- [5] The AP/WLC (MAG) provisions the corresponding QoS and replies with ADDTS Response containing authorized QoS in TSPEC.

The AP/WLC (MAG) may revise the offer to the MN based on PMIPv6 QoS reservation.

### 3.4. Case D: Network Initiated Release

QoS resources reserved for a session are released on completion of the session. When the application session completes, the policy server, or the MN may signal for the release of resources. In this use case, the network initiates the release of QoS resources.

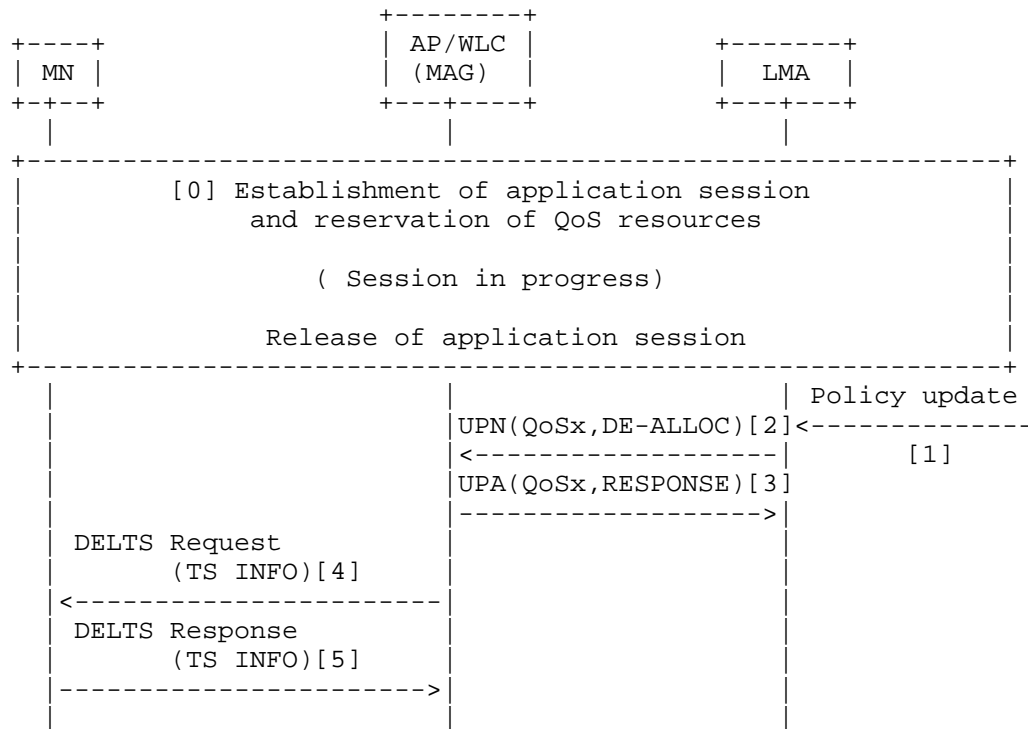


Figure 6: Network initiated QoS resource release

- [0] The MN establishes and reserves QoS resources as in use cases A, B or C.  
When the application session terminates, the policy server receives notification that the session has terminated.
- [1] LMA receives a policy update indicating that QoS for flow (QoSx) should be released. The LMA releases local resources associated with the flow.
- [2] LMA sends a UPN with QoS options - Traffic Selector field identifying the flow for which QoS resources are to be released, and operation code set to DE-ALLOCATE. No additional LMA QoS parameters are sent.
- [3] MAG replies with UPA confirming the acceptance and operation code set to RESPONSE.
- [4] AP/WLC (MAG) releases local QoS resources associated with the flow. AP/WLC derives the corresponding 802.11 Traffic Stream from the PMIPv6 Traffic Selector. The AP sends a DELTS Request

with TS INFO identifying the reservation.

[5] MN sends DELTS Response confirming release.

Since the MN has completed the session, it may send a DELTS to explicitly request release QoS resources at AP. If the AP and MN are 802.11aa capable, the release of resources may also be signaled to the MN.

### 3.5. Case E: MN Initiated Release

QoS resources reserved for a session are released on completion of the session. When the application session completes, the policy server, or the MN may signal for the release of resources. In this use case, the network initiates the release of QoS resources.

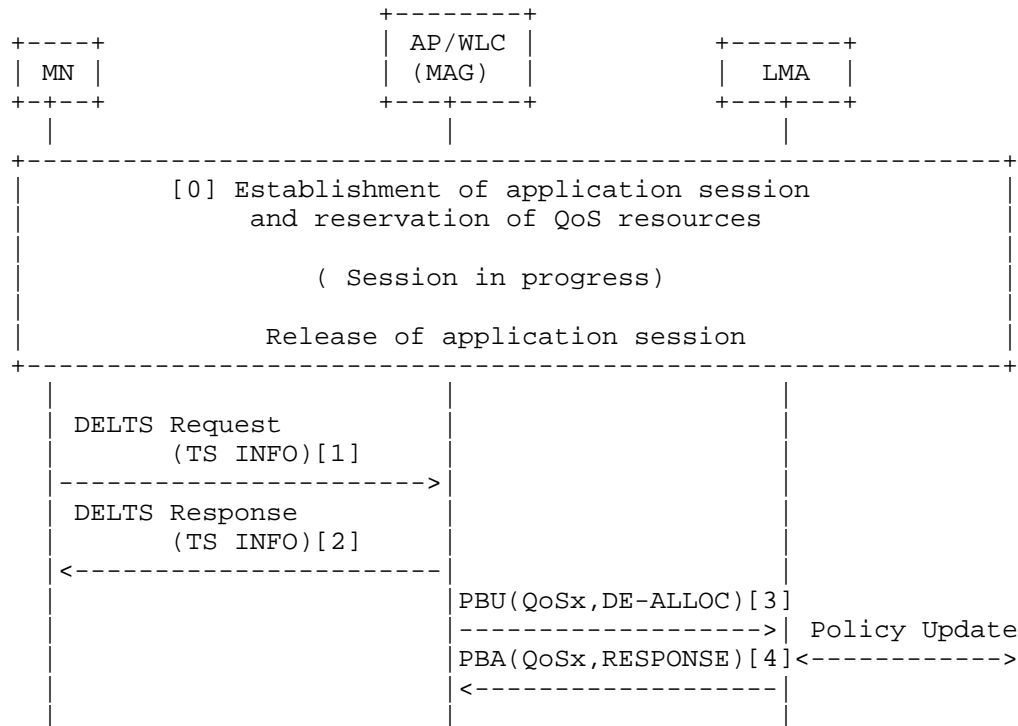


Figure 6: Network initiated QoS resource release

[0] The MN establishes and reserves QoS resources as in use cases A, B or C.

When the application session terminates, the MN prepares to release QoS resources.

- [1] MN releases its own internal resources and sends a DELTS Request to the AP/WLC with TS (Traffic Stream) INFO.
- [2] AP/WLC receives the DELTS request, releases local resources and responds to MN with a DELTS response.
- [3] AP/WLC (MAG) initiates a PBU with Traffic Selector constructed from TCLAS and PMIPv6 QoS parameters from TSPEC (QoSx) as shown in Table 1.
- [4] LMA receives the PBU, releases local resources and informs policy server. The LMA then responds with a PBA.

### 3.6. Service Guarantees in 802.11

The GBR - Guaranteed Bit Rate in mobile networks are used to request and commit resources in the network for providing the bandwidth requested. In 802.11 networks, a random backoff timer based on the access class only provides priority access to a shared medium. These mappings and recommendations allow the AP to schedule resources in a fair manner based on subscribed QoS and application request/policy server interaction.

However, there are no guaranteed or committed resources in the 802.11 network - only prioritization that gives better opportunity for frames to compete for a shared medium.

It should also be noted that unlike mobile networks which inform the MN about QoS for established or modified connections (bearers), there is no means for an MN in 802.11 networks to find out the QoS that a policy server requests to be granted. Thus, the application in MN should make its determination to downgrade a request based on SDP and media parameters to downgrade to a lower quality.

## 4. Mapping of QoS Parameters

This section outlines the handling of QoS parameters between 802.11 and PMIP QoS. 802.11 QoS reservations are made for an MN's data frames. PMIP QoS provisioning on the other hand is for IP sessions and flows. Parameters in PMIP QoS and 802.11 also need to be mapped according to the recommendations below.



#### 4.1 Connection Mapping

TSPEC in 802.11 is used to reserve QoS for a traffic stream (MN MAC, TS(Traffic Stream) id). The QoS reservation is for 802.11 frames associated with an MN's MAC address. TCLAS element with Classifier 1 (TCP/UDP Parameters) should be used to identify a flow. The flow definition should use the specification in [PMIP-QoS] Traffic Selector. Thus, there is a one-to-one mapping between the TCLAS defined flow and that in Traffic Selector.

When an 802.11 QoS reservation is complete, it is identified by a Traffic Stream (TS) identifier. This corresponds to the flow in PMIPv6 Traffic Selector, and identified in TCLAS. For releasing QoS resources identified by a PMIPv6 Traffic selector, the AP/WLC uses the above relationship to determine the corresponding TS identifier to be sent in the DELTS request.

If the MN or AP/WLC is not able to convey TCLAS, the AP/WLC should use out of band methods to determine the IP flow for which QoS is requested. This includes correlation with connection signaling protocols (e.g. 3GPP 23.402 WCS) and Traffic Selector in most recent PMIP QoS updates.

#### 4.2. QoS Class

Table 1 contains a mapping between Access Class (WMM AC) and 802.1D in 802.11 frames, and DSCP in IP data packets. The table also provides the mapping between Access Class (WMM AC) and DSCP for use in 802.11 TSPEC and PMIP QoS reservations.

QCI	DSCP	802.1D UP	WMM AC	Example Services
1	EF	6(VO)	3 AC_VO	conversational voice
2	EF	6(VO)	3 AC_VO	conversational video
3	EF	6(VO)	3 AC_VO	real-time gaming
4	AF41	5(VI)	2 AC_VI	buffered streaming
5	AF31	4(CL)	2 AC_VI	signaling
6	AF32	4(CL)	2 AC_VI	buffered streaming
7	AF21	3(EF)	0 AC_BE	interactive gaming
8	AF11	1(BE)	0 AC_BE	web access
9	BE	0(BK)	1 AC_BK	e-mail

Table 2: QoS Mapping between QCI/DSCP, 802.1D UP, WMM AC

The MN tags data packets with DSCP and 802.1D UP corresponding to the application and the subscribed policy or authorization. The AP/WLC polices sessions and flows based on these values and the QoS policy

for the MN.

For QoS reservations, TSPEC use WMM AC values and PMIP QoS uses corresponding DSCP values in Traffic Selector. 802.11 QoS Access Class AC\_VO, AC\_VI are used for QoS reservations. AC\_BE, AC\_BK should not be used in reservations.

#### 4.3. Bandwidth

There are bandwidth parameters that need to be mapped for admission controlled flows and others for non-admission controlled flows.

##### Non-Admission Controlled Flows:

Flows and sessions that do not need QoS reservation have no need for equivalent mapping for 802.11. These sessions and flows are policed by the AP/WLC to ensure that QoS policy obtained initially (during MN authorization) or dynamically over PMIP QoS is not exceeded by the MN.

All connection sessions of the MN should not in total exceed Per-MN-Agg-Max-DL-Bit-Rate and Per-MN-Agg-Max-UL-Bit-Rate in the downlink and uplink directions respectively. The non-admission controlled flows of a single connectivity session of an MN should not exceed Per-Session-Agg-Max-DL-Bit-Rate and Per-Session-Agg-Max-UL-Bit-Rate in the downlink and uplink directions respectively.

##### Admission Controlled Flows:

For flows that require reservation, the 802.11 Minimum Data Rate should be equal to Guaranteed Bit Rate (GBR). If the MN requests Minimum Data Rate in ADDTS greater than GBR, then AP/WLC should reject the admission request in ADDTS Response.

MN <--> AP/WLC(802.11)	AP/WLC(MAG) <--> LMA PMIPv6
Minimum Data Rate, DL	Guaranteed-DL-Bit-Rate
Minimum Data Rate, UL	Guaranteed-UL-Bit-Rate
Mean Data Rate UL/DL	[a]
Peak Data Rate, DL	Aggregate-Max-DL-Bit-Rate
Peak Data Rate, UL	Aggregate-Max-UL-Bit-Rate

NOTE[a] AP/WLC may derive Mean Data Rate from Minimum and Maximum Data Rates. There is no equivalent parameter in PMIP QoS.

Table 3: Bandwidth Parameters for Admission Controlled Flows

During the QoS reservation procedure, if the MN requests Minimum Data Rate, or other parameters in excess of values authorized in PMIP QoS, the AP/WLC should deny the request in ADDTS Response. Bandwidth of admission controlled flows are policed according to the mappings in Table 2.

#### 4.4. Preemption Priority

Mobile networks with resource reservation configure ARP (Allocation Retention Priority) during authorization and it is obtained in [PMIP QoS]. There is no corresponding configuration in 802.11 QoS. However, the AP/WLC may use ARP to determine priority during call setup and vulnerability to release of reserved QoS resources.

Parameter Allocation-Retention-Priority and sub fields of Priority, Preemption-Capability and Preemption-Vulnerability are used as defined in [PMIP-QoS].

When a new ADDTS request for reservation of QoS resources arrives, if there is sufficient free resources, the AP/WLC proceeds to allocate it. If there are insufficient resources, the AP/WLC may preempt existing calls based on the Preemption-Capability of the new call and Preemption-Vulnerability of established calls.

If the AP/WLC determines that an established flow with reserved resources should be released, the AP/WLC should inform the MN using ADDTS (802.11aa) and signal the LMA with a revised QoS reservation in PBU/PBA.

#### 5. Security Considerations

This document describes mapping of 3GPP QoS profile and parameters to IEEE 802.11 QoS parameters. No security concerns are expected as a result of using this mapping.

## 6. IANA Considerations

No IANA assignment of parameters are required in this document.

## 7. References

### 7.1. Normative References

- [KEYWORDS] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC1776] Crocker, S., "The Address is the Message", RFC 1776, April 1 1995.
- [TRUTHS] Callon, R., "The Twelve Networking Truths", RFC 1925, April 1 1996.

### 7.2. Informative References

- [EVILBIT] Bellovin, S., "The Security Flag in the IPv4 Header", RFC 3514, April 1 2003.
- [RFC5513] Farrel, A., "IANA Considerations for Three Letter Acronyms", RFC 5513, April 1 2009.
- [RFC5514] Vyncke, E., "IPv6 over Social Networks", RFC 5514, April 1 2009.
- [PMIP-QoS] Liebsch, et al., "Quality of Service Option for Proxy Mobile IPv6", draft-ietf-netext-pmip6-qos-11, Feb 2014.
- [WMM 1.2.0] Wi-Fi Multimedia Technical Specification (with WMM-Power Save and WMM-Admission Control) Version 1.2.0
- [802.11aa] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, Amendment 2: MAC Enhancements for Robust Audio Video Streaming, IEEE 802.11aa-2012.
- [802.11-2012] 802.11-2012 - IEEE Standard for Information technology-Telecommunications and information exchange between

systems Local and metropolitan area networks--Specific  
requirements Part 11: Wireless LAN Medium Access Control  
(MAC) and Physical Layer (PHY) Specifications

- [GSMA-IR34] Inter-Service Provider Backbone Guidelines 5.0, 22  
December 2010
- [RFC 2211] Wroclawski, J., "Specification of the Controlled Load  
Quality of Service", RFC 2211, September 1997.
- [RFC 2212] Shenker, S., Partridge, C., and R. Guerin, "Specification  
of Guaranteed Quality of Service", RFC 2212, September  
1997.
- [RFC 2216] Shenker, S., and J. Wroclawski, "Network Element QoS  
Control Service Specification Template", RFC 2216,  
September 1997.
- [TS23.107] Quality of Service (QoS) Concept and Architecture, Release  
10, 3GPP TS 23.107, V10.2.0 (2011-12).
- [TS23.207] End-to-End Quality of Service (QoS) Concept and  
Architecture, Release 10, 3GPP TS 23.207, V10.0.0 (2011-  
03).
- [TS23.402] Architecture Enhancements for non-3GPP accesses (Release  
12), 3GPP TS 23.402, V12.2.0 (2013-09).
- [TS23.203] Policy and Charging Control Architecture, Release 11, 3GPP  
TS 23.203, V11.2.0 (2011-06).
- [TS29.212] Policy and Charging Control over Gx/Sd Reference Point,  
Release 11, 3GPP TS 29.212, V11.1.0 (2011-06).
- [TS29.273] 3GPP EPS AAA interfaces (Release 12), 3GPP TS 29.273  
v12.1.0 (2013-09)

#### Authors' Addresses

John Kaippallimalil  
5340 Legacy Drive, Suite 175  
Plano, Texas 75024

E-Mail: john.kaippallimalil@huawei.com

Rajesh Pazhyannur  
170 West Tasman Drive  
San Jose, CA 95134

E-Mail: rpazhyan@cisco.com

Parviz Yegani  
1194 North Mathilda Ave.  
Sunnyvale, CA 94089-1206

E-Mail: pyegani@juniper.net

## Appendix A: QoS in 802.11, PMIPv6 and 3GPP Networks

### A.1. QoS in IEEE 802.11 Networks

IEEE 802.11-2012 [802.11-2012] provides an enhancement of the MAC layer in 802.11 networks to support QoS--EDCA (Enhanced Distributed Channel Access). EDCA uses a contention based channel access method to provide differentiated, distributed access using eight different UPs (User Priorities). EDCA also defines four access categories (AC) that provide support for the delivery of traffic. In EDCA, the random back-off timer and arbitration inter-frame space is adjusted according to the QoS priority. Frames with higher priority AC have shorter random back-off timers and arbitration inter-frame spaces. Thus, there is a better chance for higher priority frames to be transmitted. The Wi-Fi Alliance has created a specification referred to as WMM (Wi-Fi Multimedia) based on above.

The MN uses ADDTS (Add Traffic Specs) to setup QoS for a traffic stream between itself and the AP, and DELTS to delete that stream. In WMM [WMM 1.2.0], the AP advertises if admission control is mandatory for an access class. Admission control for best effort or background access classes is not recommended. The Wi-Fi Alliance has created a specification referred to as WMM-AC (Wi-Fi Multimedia Admission Control) based on the above.

### A.2. QoS in PMIPv6 Mobility domain

[PMIP-QoS] defines a mobility option that can be used by the mobility entities in the Proxy Mobile IPv6 domain to exchange Quality of Service parameters associated with an MN's IP flows. Using the QoS option, the local mobility anchor and the mobile access gateway can

exchange available QoS attributes and associated values. QoS attributes include node and mobile session Aggregate Maximum Bit Rate (AMBR) for upstream and downstream, Guaranteed Bit Rate (GBR) for upstream and downstream, Maximum Bit Rate (MBR) for upstream and downstream and the Allocation Retention Priority (ARP).

[PMIP-QoS] does not explicitly describe how the QoS signaling and QoS sub-options map into corresponding signaling and parameters in the 802.11 access network. This mapping and the procedures in the 802.11 network to setup procedures are the focus of this document. The end-to-end flow spanning 802.11 access and PMIPv6 domain and the QoS parameters in both segments are described in subsequent sections.

### A.3. QoS in 3GPP Networks

3GPP has standardized QoS for EPC (Enhanced Packet Core) from Release 8 [TS 23.107]. 3GPP QoS policy configuration defines access agnostic QoS parameters that can be used to provide service differentiation in multi vendor and operator deployments. The concept of a bearer is used as the basic construct for which the same QoS treatment is applied for uplink and downlink packet flows between the MN (host) and gateway [TS23.402]. A bearer may have more than one packet filter associated and this is called a Traffic Flow Template (TFT). The IP five tuple (IP source address, port, IP destination, port, protocol) identifies a flow.

The access agnostic QoS parameters associated with each bearer are QCI (QoS Class Identifier), ARP (Allocation and Retention Priority), MBR (Maximum Bit Rate) and optionally GBR (Guaranteed Bit Rate). QCI is a scalar that defines packet forwarding criteria in the network. Mapping of QCI values to DSCP is well understood and GSMA has defined standard means of mapping between these scalars [GSMA-IR34].

The use cases in subsequent sections use 3GPP policy along with PMIP QoS for provisioning of QoS in the 802.11 network. However, this is exemplary and alternative policy architectures may be used in practice.

NETEXT WG  
Internet-Draft  
Intended status: Standards Track  
Expires: August 18, 2014

R. Pazhyannur  
S. Speicher  
S. Gundavelli  
Cisco  
J. Korhonen  
Broadcom  
February 14, 2014

Civic Location ANI Suboption for PMIPv6  
draft-pazhyannur-netext-civic-location-ani-subopt-01.txt

Abstract

This specification defines extensions to Access Network Identifier mobility option for carrying the Civic Location information and MAG Group Identifier from the mobile access gateway to the local mobility anchor. This specification also defines a new ANI update timer suboption that enables a MAG to communicate when the MAG will update the ANI information. This helps the LMA determine the freshness of the ANI options.

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 August 18, 2014.

Copyright Notice

Copyright (c) 2014 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 and Terminology . . . . .	4
2.1. Conventions . . . . .	4
2.2. Terminology . . . . .	4
3. Civic-Location Sub-Option . . . . .	4
4. MAG Group-Id Sub-Option . . . . .	5
5. ANI Update-Timer Sub-Option . . . . .	6
6. Usage Example . . . . .	7
7. IANA Considerations . . . . .	8
8. Security Considerations . . . . .	9
9. Acknowledgements . . . . .	10
10. References . . . . .	10
10.1. Normative References . . . . .	10
10.2. Informative References . . . . .	10
Authors' Addresses . . . . .	10

## 1. Introduction

In many deployments, the LMA needs to be aware of various identifiers of client's access network to ensure appropriate policies are implemented. For example, the LMA may provide access network identifiers to location based applications. [RFC6757] defined new mobility options to enable a MAG to provide Access Network Information (ANI). In Wi-Fi systems the ANI mobility option may carry the identifier of the Access Point (for instance the BSSID, AP-Name, or the geo-spatial coordinates of the Access Point). When a client associates with an Access Point, the MAG (corresponding to the AP) may send the ANI (like SSID, BSSID, Geo-location) to the LMA.

In many deployments (especially indoor AP deployments), it is difficult to provide Geo-spatial coordinates of APs. However, for many location based applications the civic location is sufficient. To provide civic location information, this document defines a new ANI sub-option within the ANI mobility option defined in [RFC6757]. [RFC4776] provides further motivations on usage of civic information in providing human-usable information, particularly within buildings.

We also address an aspect related to ANI, frequency of ANI Update. In other words, how often does the MAG update the ANI. To understand this better, it is instructive to look at this closely in two Wi-Fi deployment scenarios:

**MAG is co-located with the Access Point:** In this scenario, whenever the Wi-Fi client hands over from a source Access Point to a target Access Point there is new Proxy Binding Update (PBU) sent by the MAG on the target AP. If the PBU contains ANI information related to BSSID, or Geo-Location then those will correspond to that of the target Access Point. As a result, the LMA has the latest ANI.

**MAG is not co-located with Access Point:** An example of such a deployment is when the MAG may be co-located with a Wireless LAN Controller (WLC) also known as an Access Controller (as defined in [RFC5415] and [RFC5416]) or it may be co-located with an Access Router. Additionally in these deployments, the Mobile Node mobility between Access Points may be handled by access network (layer 2) specific methods and may not require any PMIPv6 signaling. Specifically, there may be no need for MAG to trigger a PBU when a client hands over from one AP another AP. As a result, in these cases it is possible (depending on which ANI sub options were sent by the MAG), the LMA may have "stale" access network identifiers. For example, the LMA may contain the BSSID or Geo-Location of a previously associated AP and not the currently associated AP.

If the network deployment and applications that use ANI require the

LMA to have the current ANI, then one way of solving this problem is to require the MAG to send a fresh PBU (with updated ANI) whenever it is aware of an ANI change. This is an acceptable solution when the MAG is aggregating a small number (say between 1 and 4) APs. Consider a Wi-Fi deployment in stadium or in large exposition center or a large enterprise. The number of APs in such venues could be multiple hundred APs. This combined with a large number of mobility events may create a large number of ANI updates (sent in PBUs). In this specification, we propose a way to mechanism to specify the ANI update interval based on the deployment needs as well as the capability of the MAG and LMA.

This specification enables extensions to Access Network Identifier mobility option for carrying Location information of the mobile node from the mobile access gateway to the local mobility anchor. This documents defines a new ANI sub-option that enables a MAG to communicate how often the MAG will update the ANI information. This helps the LMA determine whether the ANI informaiton is fresh or stale.

## 2. Conventions and 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 [RFC5213] and [RFC5844].

## 3. Civic-Location Sub-Option

The Civic-Location is a mobility sub-option carried in the Access Network Identifier option defined in [RFC6757]. This sub-option carries the Civic Location information of the mobile node as known to the MAG. The format of this option is defined below.

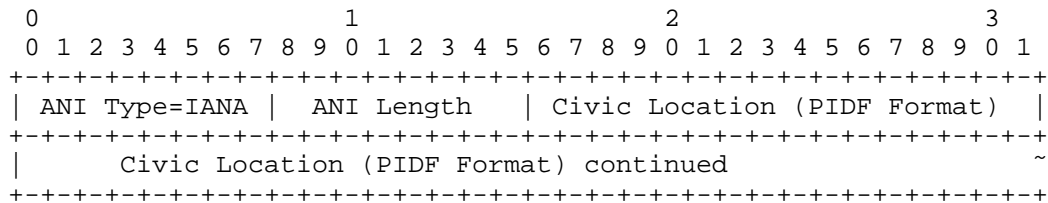


Figure 1: Network-Identifier Sub-option

ANI Type: <IANA-1>

ANI Length: Total length of this sub option in octets, excluding the ANI Type and ANI length fields.

Civic Location: This format is as specified in the Presence Information Data Format Location Object [RFC5139] with the additional constraint that the length shall not exceed 255 bytes. System architectures may choose to identify the exact PIDF XML elements to be carried in the PIDF object.

#### 4. MAG Group-Id Sub-Option

In many deployments, MAGs may be co-located with APs. In such cases, APs may be clustered in a "group". There is a common policy (for QoS, charging, etc) for all MNs connected to the same group. Further, in some cases there is a common policy (for QoS, DPI, etc) between MAGs and LMA in the same group. The group identifier may also serve a proxy for coarse location identification for MNs connected to the group of MAGs. These considerations motivate introduction of a group identifier to a MAG.

The MAG Group Identifier is a mobility sub-option carried in the Access Network Identifier option defined in [RFC6757]. The MAG Group Identifier identifies the group affiliation of the mobile access gateway within that Proxy Mobile IPv6 domain.

When the MAG is configured with a group identifier, the MAG may send its group-id in the PBU. The usage of the group identifier by the LMA is left to implementation. The format of this option is defined below.

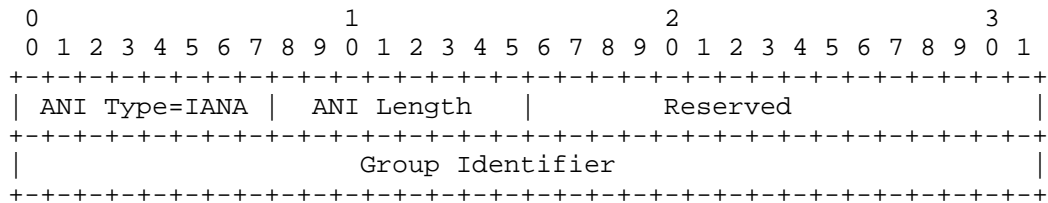


Figure 2: MAG Group-Identifier Sub-option

ANI Type: <IANA-2>

ANI Length: Total length of this sub option in octets, excluding the ANI Type and ANI length fields. The value is always 6.

Reserved: MUST be set to zero when sending and ignored when received.

Group Identifier:

## 5. ANI Update-Timer Sub-Option

The ANI Update Timer is a mobility sub-option carried in the ANI option defined in [RFC6757]. The MAG sends a PBU with an updated value of ANI mobility options when the update-timer expires. Specifically, if the update-timer expires and the ANI values are identical to the last transmitted ANI values, then a PBU shall not be transmitted.

When the Update-Timer Sub option is carried in a PBU, it is considered as a proposed value for the update-timer. When the Update-Timer sub option is carried in a PBA, then it is considered as an accepted value for the update-timer. If the MAG does not receive a update-timer sub option in PBA (in response to sending the sub-option in the PBU), then it the MAG behavior with respect to updating the ANI values is left to implementation choices.

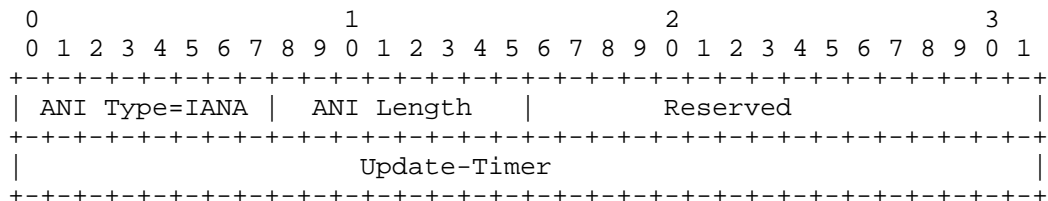


Figure 3: Network-Identifier Sub-option

ANI Type: <IANA-3>

ANI Length: Total length of this sub option in octets, excluding the ANI Type and ANI length fields is always 6.

Reserved: MUST be set to zero when sending and ignored when received.

Update-Timer: Update-Timer is a 16 bit unsigned integer. It indicates the time in seconds before the MAG sends an update value of ANI mobility options. A value of 0 indicates that the MAG will send an updated ANI mobility option as soon as it discovers a change in ANI values.

## 6. Usage Example

Consider a case where the MAG is not co-located with an AP.

- o MN Attaches to Wi-Fi Network
- o MAG registers with the LMA and provides an Update-Timer ANI sub option. The LMA responds with a value of Update-Timer in the PBA.
- o Application request LMA for ANI Information
- o if ANI information is current (for example, the MAG had sent the Update-Timer value of 0) then LMA provides ANI information
- o if ANI is not current, LMA sends Update Notification with ANI-Update-Required Notification reason
- o MAG sends a re-registration with updated ANI sub options

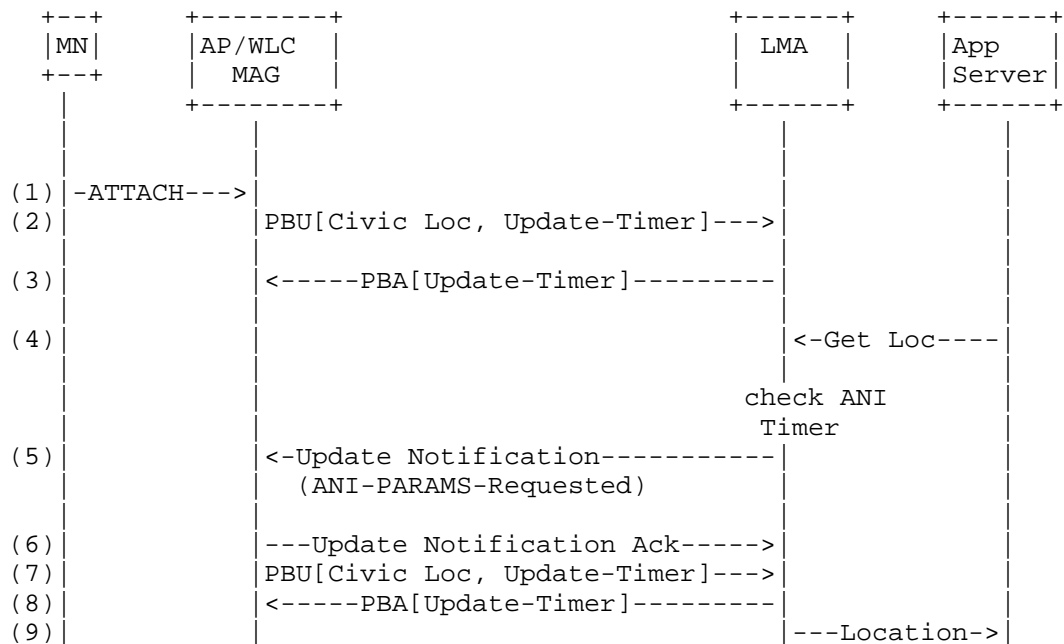


Figure 4: Usage Example

Note the the protocol for retrieving location from the LMA is outside the scope of this document.

## 7. IANA Considerations

This document requires the following IANA action.

- o Action-1: This specification defines a new Access Network Identifier sub-option called Civic Location Sub-option. This mobility sub-option is described in Section 3 and this sub-option can be carried in Access Network Identifier mobility option. The type value <IANA-1> for this sub-option needs to be allocated from the registry "Access Network Information (ANI) Sub-Option Type Values". RFC Editor: Please replace <IANA-1> in Section 3 with the assigned value, and update this section accordingly.
- o Action-2: This specification defines a new Access Network Identifier sub-option called MAG Group Identifier Sub-option. This mobility sub-option is described in Section 4 and this sub-option can be carried in Access Network Identifier mobility option. The type value <IANA-2> for this sub-option needs to be allocated from the registry "Access Network Information (ANI) Sub-

Option Type Values". RFC Editor: Please replace <IANA-2> in Section 4 with the assigned value, and update this section accordingly.

- o Action-3: This specification defines a new Access Network Identifier sub-option called ANI-Update-Frequency Sub-option. This mobility sub-option is described in Section 5 and this sub-option can be carried in Access Network Identifier mobility option. The type value <IANA-3> for this sub-option needs to be allocated from the registry "Access Network Information (ANI) Sub-Option Type Values". RFC Editor: Please replace <IANA-3> in Section 5 with the assigned value, and update this section accordingly.

## 8. Security Considerations

The Civic Location and the ANI-Update-Frequency sub-Options defined in this specification are to be carried in the Access Network Identifier option defined in [RFC6757]. This sub-option is carried in Proxy Binding Update and Proxy Binding Acknowledgement messages. This sub-option is carried like any other Access Network Identifier sub-option as defined in [RFC6757]. Therefore, it inherits from [RFC5213] and [RFC6757], its security guidelines and does not require any additional security considerations.

The Civic Location sub-option carried in the Access Network Information option exposes the geo-location of the network to which the mobile node is attached. This information is considered to be very sensitive, so care must be taken to secure the Proxy Mobile IPv6 signaling messages when carrying this sub-option. The base Proxy Mobile IPv6 specification [RFC5213] specifies the use of IPsec for securing the signaling messages, and those mechanisms can be enabled for protecting this information. Operators can potentially apply IPsec Encapsulating Security Payload (ESP) with confidentiality and integrity protection for protecting the location information.

Access-network-specific information elements that the mobile access gateway sends may have been dynamically learned over DHCP or using other protocols. If proper security mechanisms are not in place, the exchanged information may be potentially compromised with the mobile access gateway sending incorrect access network parameters to the local mobility anchor. This situation may potentially result in incorrect service policy enforcement at the local mobility anchor and impact to other services that depend on this access network information. This threat can be mitigated by ensuring the communication path between the mobile access gateway and the access points is properly secured by the use of IPsec, Transport Layer



Security (TLS), or other security protocols.

## 9. Acknowledgements

TBD

## 10. References

### 10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.
- [RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.
- [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.
- [RFC6757] Gundavelli, S., Korhonen, J., Grayson, M., Leung, K., and R. Pazhyannur, "Access Network Identifier (ANI) Option for Proxy Mobile IPv6", RFC 6757, October 2012.

### 10.2. Informative References

- [RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.
- [RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009.

Authors' Addresses

Rajesh S. Pazhyannur  
Cisco  
170 West Tasman Drive  
San Jose, CA 95134,  
USA

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

Sebastian Speicher  
Cisco  
Richtistrasse 7  
Wallisellen, Zurich, 8304  
Switzerland

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

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

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

Jouni Korhonen  
Broadcom  
Porkkalankatu 24  
Helsinki FIN-00180  
Finland

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

