

NETEXT Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: April 24, 2014

CJ. Bernardos, Ed.  
UC3M  
October 21, 2013

Proxy Mobile IPv6 Extensions to Support Flow Mobility  
draft-ietf-netext-pmipv6-flowmob-08

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.

The extensions described in this document consist on 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 April 24, 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 . . . . .	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
3.2.3. MN with combination of prefix(es) in use and new prefix(es) on each MAG . . . . .	12
4. Message Formats . . . . .	13
4.1. Home Network Prefix . . . . .	13
5. Conceptual Data Structures . . . . .	13
5.1. Multiple Proxy Care-of Address Registration . . . . .	14
5.2. Flow Mobility Cache . . . . .	14
6. Mobile Node considerations . . . . .	15
7. IANA Considerations . . . . .	16
8. Security Considerations . . . . .	16
9. Authors . . . . .	16
10. Acknowledgments . . . . .	17
11. References . . . . .	18
11.1. Normative References . . . . .	18
11.2. Informative References . . . . .	18
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 Mobile Node's (MN) attachment and providing IP connectivity. The LMA is the entity assigning one or more Home Network Prefixes (HNPs) 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.

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, 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).

### 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].

3. 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 above-mentioned scenarios. 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, Section 3.2.2 and Section 3.2.3.

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. The MN makes the final IP flow mobility decision, and then the LMA follows that decision and update its forwarding state accordingly. Note that this does not prevent network initiated mobility, the network still could 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 not by both.

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

This scenario corresponds to the use case scenario number 1 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, and the local mobility anchor does not need to send any kind of signaling in order to move flows

across the different physical interfaces.

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-1}) is defined, to allow the mobile access gateway 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 one 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.

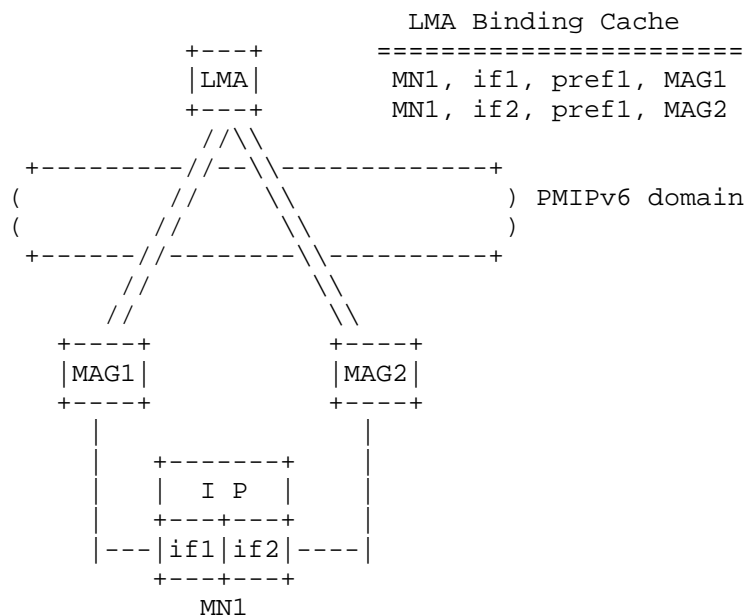


Figure 1: Shared prefix across physical interfaces scenario

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 and if2). 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 certain point, flow Y can be moved to also go through MAG1. As shown in Figure 2, no signaling between the local mobility anchor and the mobile access gateways is needed.

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.

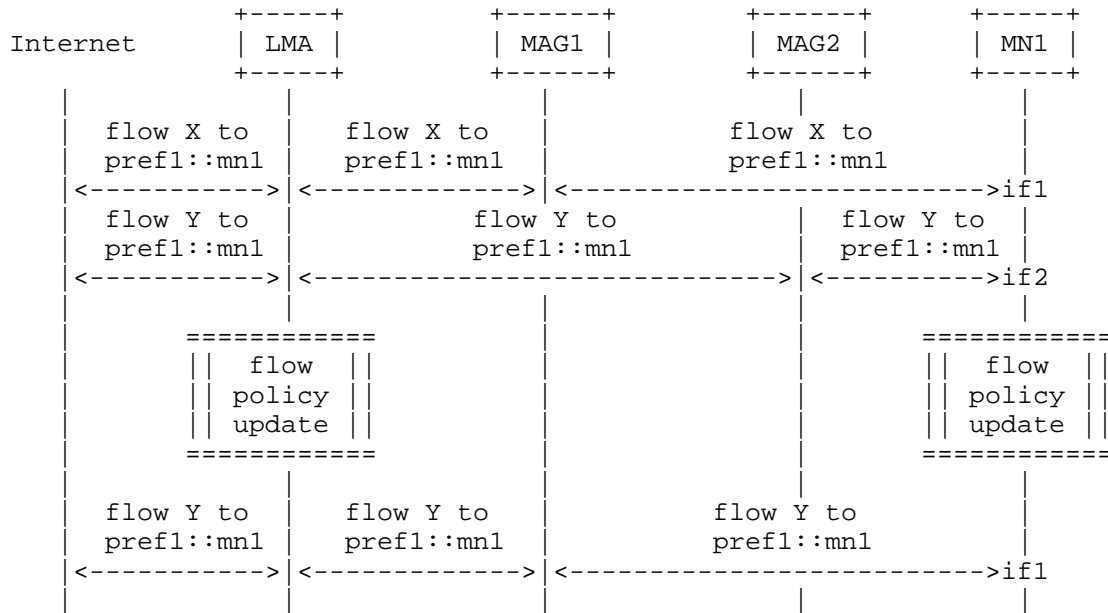


Figure 2: Flow mobility message sequence with common set of prefixes

Figure 3 shows the state of the different network entities after moving flow Y in the previous example. This documents 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.

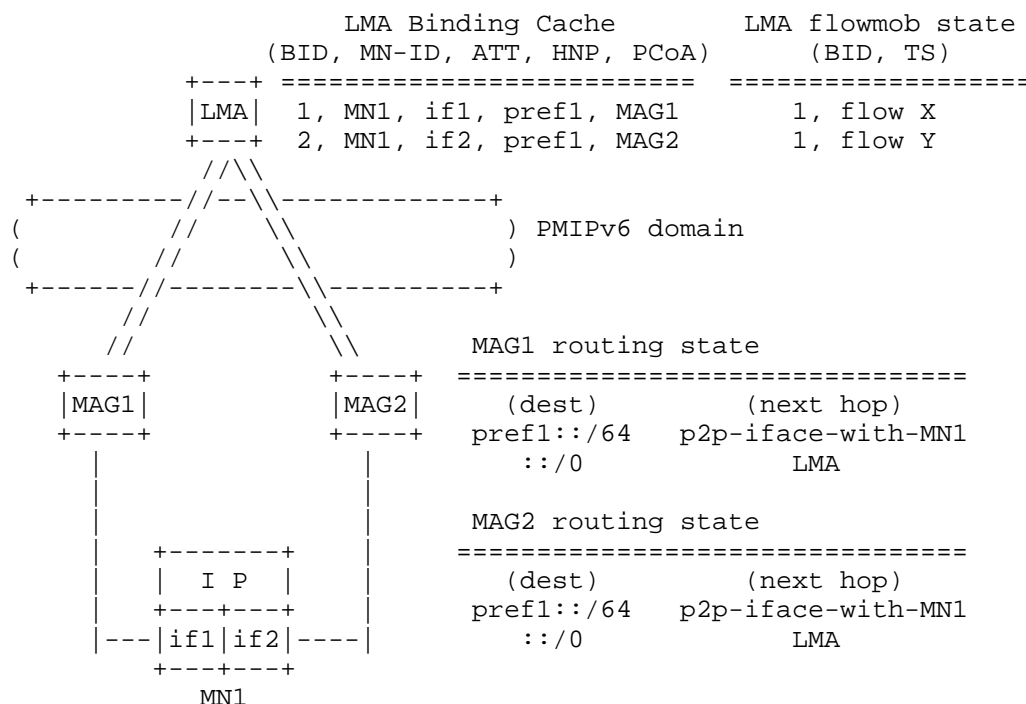


Figure 3: Data structures with common set of prefixes

### 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 and third use case 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. Two different, but related, approaches are considered next.

The first approach corresponds to the use case scenario number 2 described in Section 3.1, in which a multi-interfaced mobile node obtains a different set of prefixes on each attachment. 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 the Update Notifications for Proxy Mobile IPv6 defined in

[I-D.ietf-netext-update-notifications]. 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).

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 an Update Notification (UPN) message, of type (2) "UPDATE-SESSION-PARAMETERS" (NOTE from the Editor: a new Notification Reason value might be defined for just flow mobility purposes if it proves to be cleaner). This message includes a Home Network Prefix for each of the prefixes that 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. This UPN message has the Acknowledgement Requested Flag ('A' Flag) set to 1, so the MAG replies with an Update Notification Acknowledgement (UPA) message. The message sequence is shown in Figure 4.

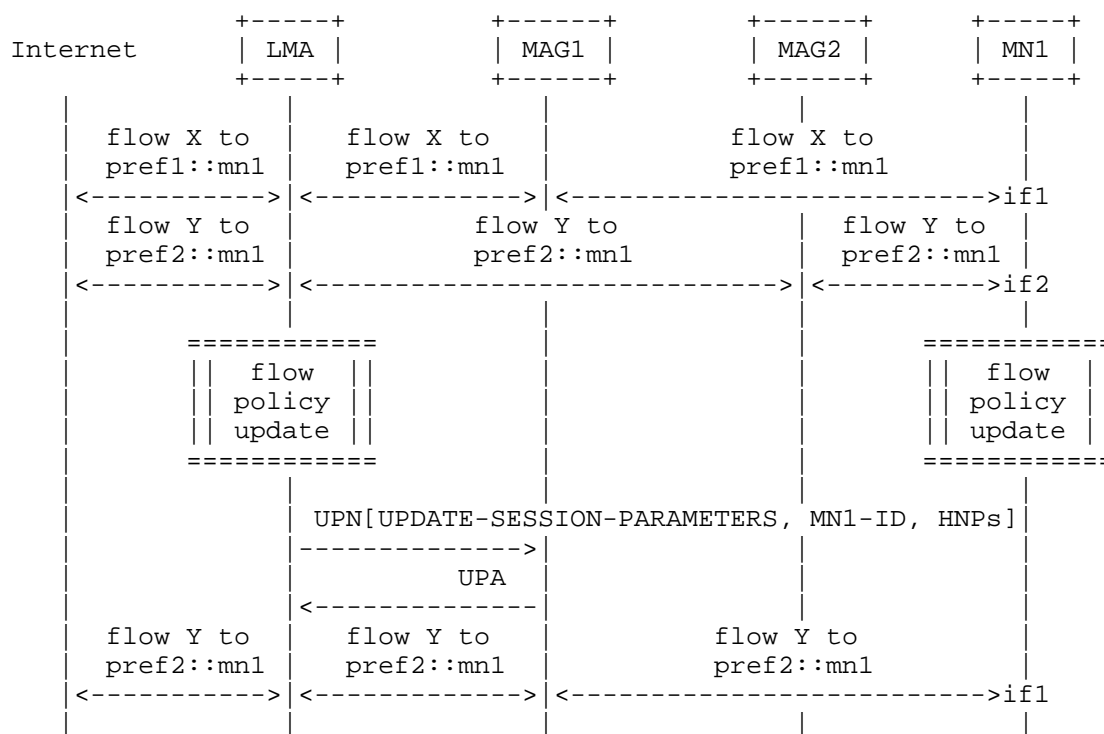


Figure 4: Flow mobility message sequence when the LMA assigns

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.

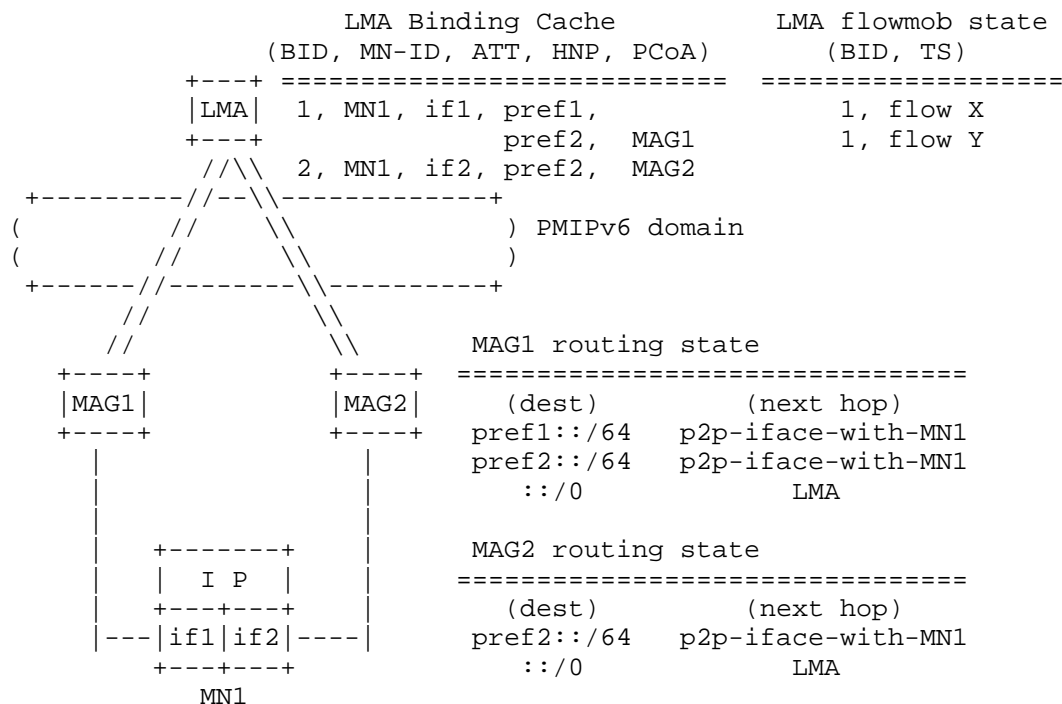


Figure 5: Data structures when the LMA assigns a different set of prefixes

The second approach corresponds to the use case scenario number 3 described in Section 3.1, in which upon new physical interface attachment, the MN obtains a combination of prefix(es) in use and new prefix(es). Here, the mobile node is already attached to the PMIPv6-Domain via MAG1. At a certain moment, the mobile node attaches a new interface (if2) to MAG2. MAG2 sends a PBU which is then used by the LMA to enable flow mobility. In this case, we consider that flows are moved with a prefix granularity, meaning that flows are moved by moving prefixes among the different MAGs the mobile node is attached to. In this example, flow Y is bound to pref2::/64 and therefore the flow can be moved by just binding pref2::/64 to MAG2. This is done by including the prefix in the PBA message. The scenario is shown in Figure 6.

Optionally, a Binding Revocation Indication message [RFC5846] with

the P bit set MAY be sent to MAG1 to indicate that this is a revocation of PMIP prefix(es). After processing BRI, the source MAG MUST send a Binding Revocation Acknowledgement (BRA) message back to the LMA.

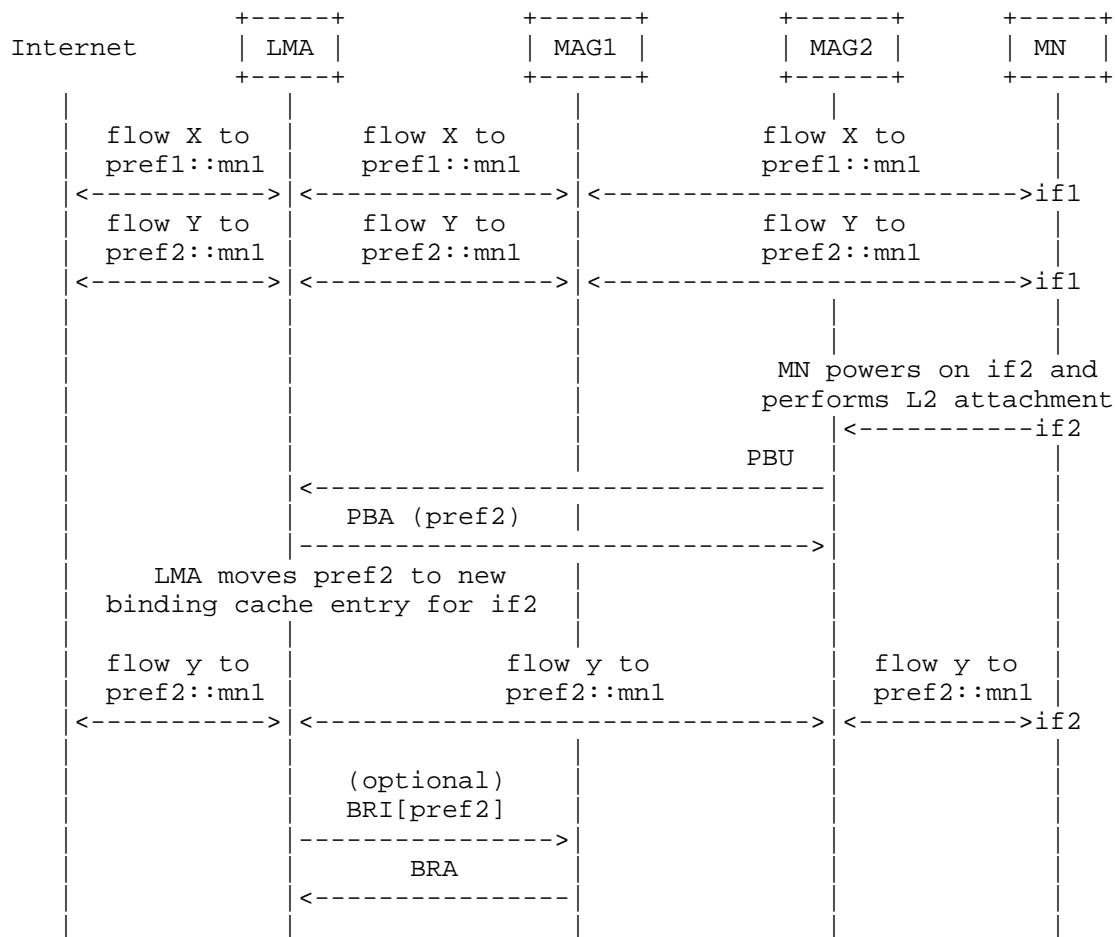


Figure 6: Flow mobility message sequence with different set of prefixes per physical interface (PBU signaling)

### 3.2.3. MN with combination of prefix(es) in use and new prefix(es) on each MAG

This scenario is a hybrid of the ones described in Section 3.2.1 and Section 3.2.2. It requires flow mobility signaling to enable relocating flows for the new prefix(es) which are not shared across

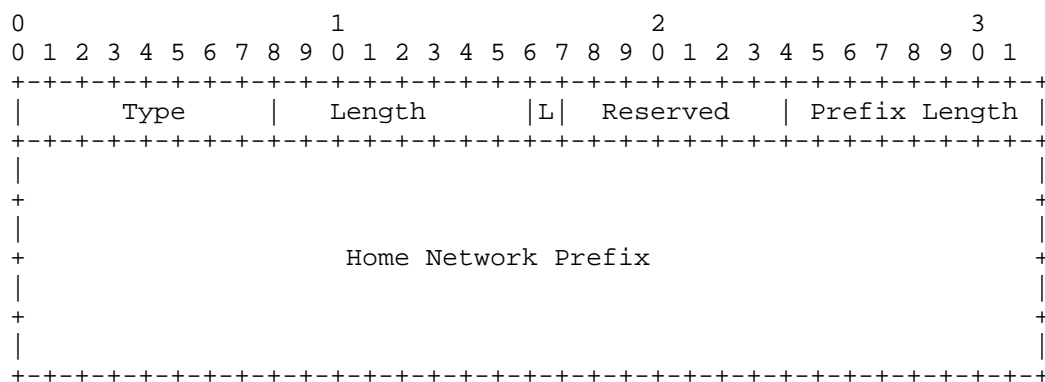
attachments.

#### 4. Message Formats

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

##### 4.1. Home Network Prefix

A new flag (L) is included in the Home Network Prefix mobility 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 mobility 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.

#### 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 addresses 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 7: Extended Binding Cache

Figure 7 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 bounded 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 8. 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 8: 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 basing 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 deregistered.

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 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.

## 7. IANA Considerations

This specification defines a new value for the Handoff Indicator {IANA-1} and a new flag (L) in the Home Network Mobility Option.

## 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 [I-D.ietf-netext-update-notifications].

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: Kchowdhu@cisco.com

Vijay Devarapalli

E-mail: vijay@wichorus.com

Sri Gundavelli

E-mail: sgundave@cisco.com

Youn-Hee Han

E-mail: yhhan@kut.ac.kr

Yong-Geun Hong

E-mail: yonggeun.hong@gmail.com

Mohana Dahamayanthi Jeyatharan

E-mail: mohana.jeyatharan@sg.panasonic.com

Rajeev Koodli

E-mail: rkoodli@cisco.com

Kent Leung

E-mail: kleung@cisco.com

Telemaco Melia

E-mail: Telemaco.Melia@alcatel-lucent.com

Bruno Mongazon-Cazavet

E-mail: Bruno.Mongazon-Cazavet@alcatel-lucent.com

Chan-Wah Ng

E-mail: chanwah.ng@sg.panasonic.com

Behcet Sarikaya

E-mail: sarikaya@ieee.org

Tran Minh Trung

E-mail: trungtm2909@gmail.com

Frank Xia

E-mail: xiayangsong@huawei.com

## 10. Acknowledgments

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

The authors would also like to thank Marco Liebsch and Juan-Carlos Zuniga for their reviews of this document.

The work of Carlos J. Bernardos has also been partially supported by the European Community's Seventh Framework Programme under grant agreement n. FP7-317941 (iJOIN project).

## 11. References

### 11.1. Normative References

- [I-D.ietf-netext-update-notifications]  
Krishnan, S., Gundavelli, S., Liebsch, M., Yokota, H., and J. Korhonen, "Update Notifications for Proxy Mobile IPv6", draft-ietf-netext-update-notifications-12 (work in progress), October 2013.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.
- [RFC5846] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K., and P. Yegani, "Binding Revocation for IPv6 Mobility", RFC 5846, June 2010.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.
- [RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

### 11.2. Informative References

- [I-D.ietf-netext-logical-interface-support]  
Melia, T. and S. Gundavelli, "Logical Interface Support for multi-mode IP Hosts", draft-ietf-netext-logical-interface-support-08 (work in progress), October 2013.

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/>



Netext  
Internet-Draft  
Intended status: Informational  
Expires: April 24, 2014

Ravi. Valmikum  
Unaffiliated  
Rajeev. Koodli  
Cisco Systems  
October 21, 2013

EAP Attributes for WiFi - EPC Integration  
draft-ietf-netext-wifi-epc-eap-attributes-04

## Abstract

With WiFi beginning to establishing itself as a trusted access network for service providers, it has become important to provide functions commonly available in 3G and 4G networks in WiFi access networks. Such functions include Access Point Name (APN) Selection, multiple Packet Data Network (PDN) connections and seamless mobility between WiFi and 3G/4G networks.

EAP/AKA (and EAP/AKA') is standardized by 3GPP as the access authentication protocol for trusted access networks. This IETF specification is required for mobile devices to access the 3GPP Evolved Packet Core (EPC) networks. This document defines a few new EAP attributes and procedures to provide the above-mentioned functions in trusted WiFi access networks.

## Status of this Memo

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

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

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

This Internet-Draft will expire on April 24, 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
1.1. APN Selection . . . . .	3
1.2. Multiple APN Connectivity . . . . .	4
1.3. WiFi to EUTRAN mobility . . . . .	4
2. Reference Architecture and Terminology . . . . .	4
3. Protocol Overview . . . . .	4
3.1. Brief Introduction to EAP . . . . .	4
3.2. 802.11 Authentication using EAP over 802.1X . . . . .	5
4. Protocol Extensions . . . . .	7
4.1. APN Selection . . . . .	7
4.2. WiFi to UTRAN/EUTRAN Mobility . . . . .	7
4.3. Connectivity Type . . . . .	8
5. Attribute Extensions . . . . .	8
5.1. AT_VIRTUAL_NETWORK_ID . . . . .	8
5.2. AT_VIRTUAL_NETWORK_REQ . . . . .	9
5.3. AT_CONNECTIVITY_TYPE . . . . .	9
5.4. AT_HANDOVER_INDICATION . . . . .	10
5.5. AT_HANDOVER_SESSION_ID . . . . .	11
6. Security Considerations . . . . .	11
7. IANA Considerations . . . . .	12
8. Acknowledgment . . . . .	12
9. Informative References . . . . .	12
Appendix A. Change Log . . . . .	13
Authors' Addresses . . . . .	13

## 1. Introduction

The convergence of multiple access technologies is becoming more reality now than ever. Specifically, WiFi has emerged as a trusted access technology for mobile service providers. It has become important to provide certain functions in WiFi which are commonly supported in licensed-spectrum networks such as 3G and 4G networks. This draft specifies a few new EAP attributes and procedures for a Mobile Node (MN) to interact with the network to support some of the functions (see below). These new attributes serve as a trigger for network nodes to undertake the relevant mobility operations. For instance, when the Mobile Node indicates and the network agrees for a new IP session (i.e., a new APN in 3GPP), the corresponding attribute (defined below) can act as a trigger for the Mobile Anchor Gateway (MAG) to initiate a new mobility session with the Local Mobility Anchor (LMA).

The 3GPP networks support many functions that are not commonly implemented in a WiFi network. This draft specifically addresses the following functions and specifies methods to implement them using EAP-AKA' [RFC5448] and EAP-AKA [RFC4187]. Since the attributes share the same IANA registry, the methods are applicable to EAP-AKA', EAP-AKA and EAP-SIM [RFC4186], and with appropriate extensions, are possibly applicable for other EAP methods as well.

The following sections will focus on implementation of the following functions in the context of a 802.1X/EAP based WiFi network.

- o APN Selection
- o Multiple APN Connectivity
- o WiFi to 3G/4G (UTRAN/EUTRAN) mobility

EAP [RFC3748] is widely deployed in access networks to authenticate the user during network attach, and periodically afterwards. Apart from being an authentication mechanism, EAP provides a conduit to propagate information between a MN and network elements such as a WiFi Access Controller. Each of the addressed functions is described in detail below.

### 1.1. APN Selection

The 3GPP networks support the concept of an APN (Access Point Name). This is defined in [GPRS]. Each APN is an independent IP network with it's own set of IP services. When the MN attaches to the network, it may select a specific APN to receive desired services. For example, to receive generic internet services, user device may select APN "Internet" and to receive IMS voice services, it may select APN "IMSvoice".

In a WiFi access scenario, a MN needs a way of sending the desired APN name to the network. This draft specifies a method to propagate the APN information via EAP.

### 1.2. Multiple APN Connectivity

As an extension of APN Selection, a MN may choose to connect to multiple IP networks simultaneously. 3GPP provides this feature via Additional PDP contexts or Additional PDN connections. The 3GPP defines extensive set of signaling procedures to implement these features. In a trusted WiFi network, a MN connects to the first APN via DHCPv4 or IPv6 Router Solicitation. For subsequent APN connections, a procedure is needed, which is expected to be standardized by 3GPP in its Release-12 specification.

### 1.3. WiFi to EUTRAN mobility

When operating in a multi-access network, a MN may want to gracefully handover it's IP attachment from one access to another. For instance, a MN connected to 3GPP EUTRAN network may choose to move its connectivity to a trusted WiFi network. Alternatively, the MN may choose to connect from both the access technologies simultaneously, and maintain two independent IP attachments. To implement these scenarios, the MN needs a way to indicate seamless handover as well as a means to correlate the UTRAN/EUTRAN session with the new WiFi session. This draft specifies a method to propagate EUTRAN session identification (GUTI) to the network via EAP. This helps the network to correlate the sessions between the two RAN technologies and implement a handover.

## 2. Reference Architecture and 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].

## 3. Protocol Overview

### 3.1. Brief Introduction to EAP

EAP is defined as a generic protocol in [RFC3748]. EAP, combined with one of the payload protocols such as EAP-AKA' [RFC5448] can accomplish several things in a network:

- o Establish identity of the user (MN) to the network.
- o Authenticate the user during the first attach with the help of an authentication center that securely maintains the user credentials. This process is called EAP Authentication.
- o Re-authenticate the user periodically, but without the overhead of a round-trip to authentication center. This process is called EAP Fast Re-Authentication.

This draft makes use of the EAP Authentication procedure to implement the above-mentioned functions. The use of EAP Fast Re-Authentication procedure is for further study. Both the EAP Authentication and EAP Fast Re-Authentication procedures are specified for trusted access network use in 3GPP [3GPP-TS-33.402]

### 3.2. 802.11 Authentication using EAP over 802.1X

In a WiFi network, EAP is carried over the IEEE 802.1X Authentication protocol. The IEEE 802.1X Authentication is a transparent, payload-unaware mechanism to carry the authentication messages between the MN and the WiFi network elements.

EAP, on the other hand, has multiple purposes. Apart from its core functions of communicating MN's identity to the network and proving MN's credentials, it also allows the MN to send arbitrary information elements to help establish the MN's IP session in the network. The following figure shows an example end-to-end EAP flow in the context of an IEEE 802.11 WiFi network.

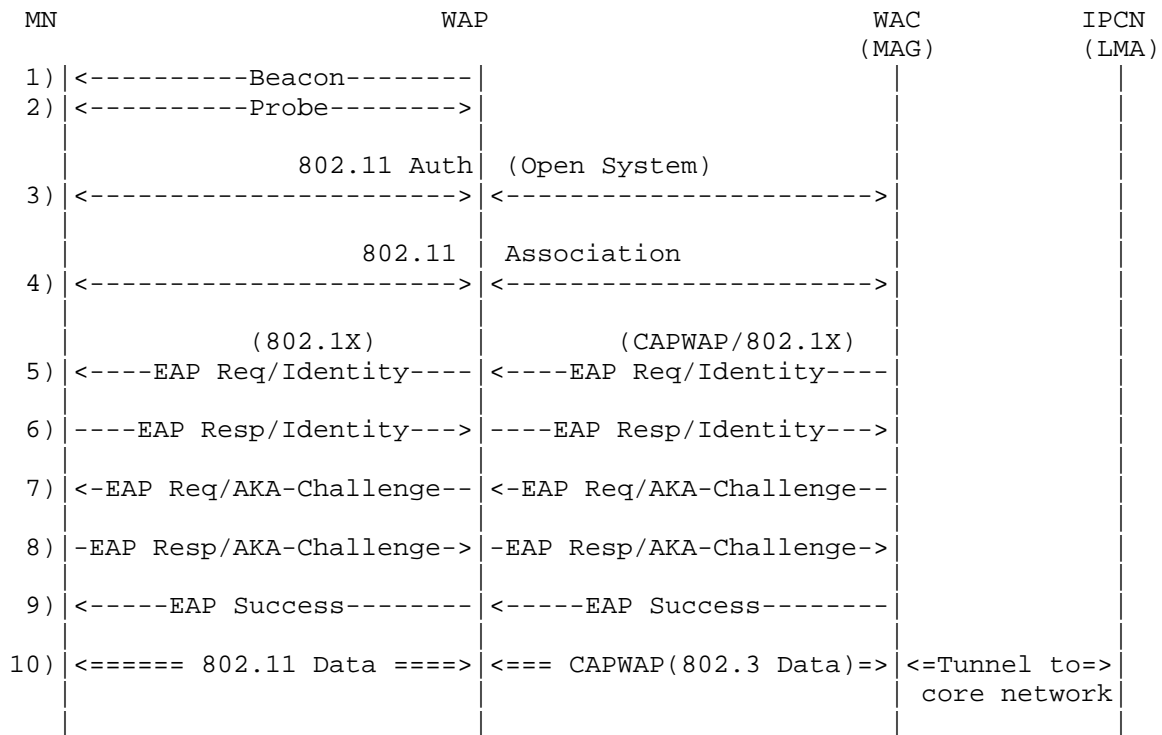


Figure 1: Example EAP Deployment

## Legend:

- o MN: Mobile Node
- o WAP: WiFi Access Point
- o WAC: WiFi Access Controller. In a PMIPv6-deployed network, hosts the MAG functionality or is assumed to have a suitable interface to the MAG. In the following, we simply use "WAC" notation. The MAG functionality within the WAC (or within the WiFi access network), or a suitable interface to MAG is assumed for PMIPv6 deployments.
- o IPCN: IP Core Network. This includes the LMA function. It generically also includes the AAA server function.
- o
- o NOTE: The figure shows separate WiFi Access Point and WiFi Access Controller, following the split-MAC model of CAPWAP [RFC5415]. A particular deployment may have the two functions within a single node.

## Call Flow Description:

1. MN detects a beacon from a WAP in the vicinity
2. MN probes the WAP to determine suitability to attach (Verify SSID list, authentication type and so on)
3. MN initiates the IEEE 802.11 Authentication with the WiFi network. In WPA/WPA2 mode, this is an open authentication without any security credential verification.
4. MN initiates 802.11 Association with the WiFi network.
5. WiFi network initiates 802.1X/EAP Authentication procedures by sending EAP Request/Identity
6. MN responds with it's permanent or temporary identity
7. WiFi network challenges the MN to prove it's credentials by sending EAP Request/AKA-Challenge
8. MN calculates the security digest and responds with EAP Response/AKA-Challenge
9. If authentication is successful, WiFi network responds to MN with EAP Success.
10. End-to-End data path is available for MN to start IP level activity (DHCPv4, IPv6 Router Solicitation etc.,)

#### 4. Protocol Extensions

The following sections define the new EAP attributes and their usage.

##### 4.1. APN Selection

In a WiFi network, a MN includes AT\_VIRTUAL\_NETWORK\_ID attribute in EAP-Response/AKA-Challenge to indicate the desired APN identity for the first PDN connection.

If the MN does not include AT\_VIRTUAL\_NETWORK\_ID attribute in EAP-Response/AKA-Challenge, the network may select an APN by other means. This selection mechanism is outside the scope of this draft.

##### 4.2. WiFi to UTRAN/EUTRAN Mobility

When a multi-access MN enters a WiFi network, if MN intends to continue the IP session previously attached via UTRAN/EUTRAN, it shall include the following parameters in the EAP-Response/AKA-Challenge.

- o AT\_HANDBOVER\_INDICATION : This attribute indicates to the network that MN intends to continue the IP session from UTRAN/EUTRAN. If a previous session can be located, network shall honor this request by connecting the WiFi access to the existing IP session.
- o AT\_HANDBOVER\_SESSION\_ID: MN may use this attribute to identify the session on UTRAN/EUTRAN. If used, this attribute shall contain P-TMSI if the previous session was on UTRAN or shall contain

M-TMSI if the previous session was on EUTRAN. This attribute helps the network correlate the WiFi session to an existing UTRAN/EUTRAN session.

#### 4.3. Connectivity Type

A Mobile Node indicates its preference for connectivity using the AT\_CONNECTIVITY\_TYPE attribute in the EAP-Response/AKA-Challenge message. The preference indicates whether the MN wishes connectivity to the Evolved Packet Core (so-called "EPC PDN connectivity") or Internet Offload (termed as "Non-Seamless Wireless Offload").

The network makes its decision and replies with the same attribute in the EAP Success message.

### 5. Attribute Extensions

#### 5.1. AT\_VIRTUAL\_NETWORK\_ID

The AT\_VIRTUAL\_NETWORK\_ID attribute identifies the virtual IP network that the MN intends to attach to. The implementation of the virtual network on the core network side is technology specific. For instance, in a 3GPP network, the virtual network is implemented based on the 3GPP APN primitive.

This attribute can be included in any of the EAP Request messages that are integrity protected, such as the EAP-Response/AKA-Challenge.

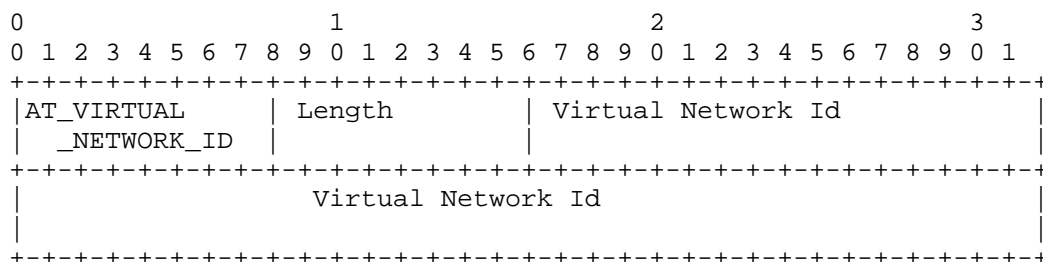


Figure 2: AT\_VIRTUAL\_NETWORK\_ID EAP Attribute

Virtual Network Id:

An arbitrary octet string that identifies a virtual network in the access technology MN is attaching to. For instance, in 3GPP EUTRAN, this could be an APN.

## 5.2. AT\_VIRTUAL\_NETWORK\_REQ

When MN intends to connect an APN, MN shall use this attribute to indicate different capabilities to the network. In turn, the network provides what is supported.

From the MN, this attribute can be included only in EAP-Response/Identity. From the network, it can be included in any suitable EAP message. In the MN-to-network direction, the Type field (below) indicates MN's request. In the network-to-MN direction, the Type field indicates network's willingness to support the request; a present Type field indicates the network support for that Type.

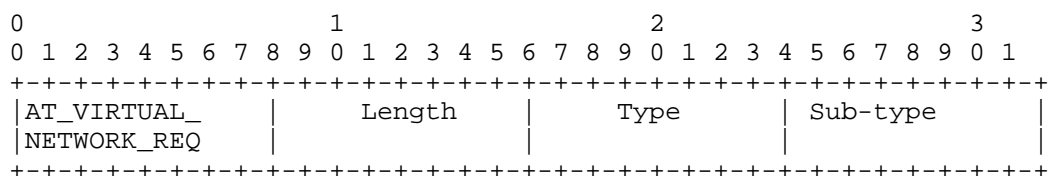


Figure 3: AT\_VIRTUAL\_NETWORK\_REQ EAP Attribute

Type:

Type shall have one of the following values:

- o 0 : Reserved
- o 1 : Single PDN connection
- o 2 : Multiple PDN connection. Can request Non-Seamless WiFi Offload or EPC connectivity (see Connectivity Type attribute below)

Sub-type:

Sub-type shall have one of the following values:

- o 0 : Reserved
- o 1 : PDN Type: IPv4
- o 2 : PDN Type: IPv6
- o 3 : PDN Type: IPv4v6

## 5.3. AT\_CONNECTIVITY\_TYPE

For Multiple PDN Connections only, a Mobile Node uses this attribute to indicate whether it wishes the connectivity type to be Non-Seamless WLAN Offload or EPC.

From the MN, this attribute can be included only in EAP-Response/

Identity. The network can include this attribute in any suitable EAP message.

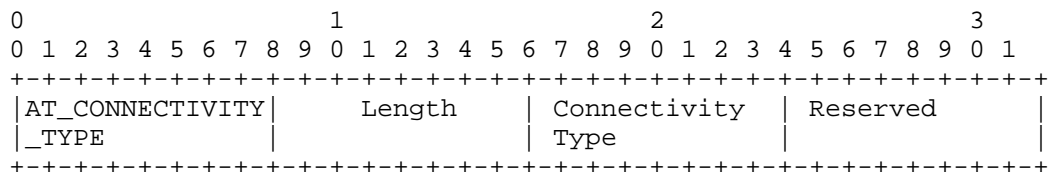


Figure 4: AT\_CONNECTIVITY\_TYPE EAP Attribute

Connectivity Type:

Connectivity Type shall have one of the following values:

- o 0 : Reserved
- o 1 : Non-Seamless WLAN Offload (NSWO)
- o 2 : EPC PDN connectivity

#### 5.4. AT\_HANDBOVER\_INDICATION

This attribute indicates a MN's handover intention of an existing IP attachment.

This attribute can be included in any of the EAP Request messages that are integrity protected, such as EAP-Response/AKA-Challenge.

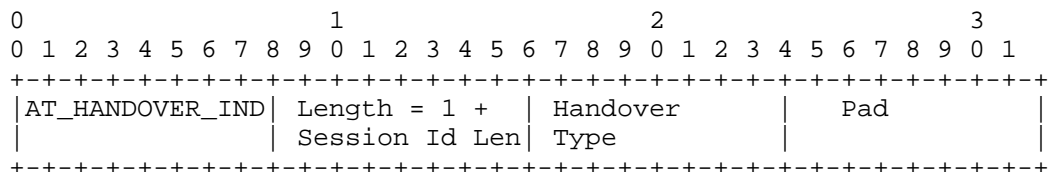


Figure 5: AT\_HANDBOVER\_INDICATION EAP Attribute

Handover Type:

- o 0 - MN has no intention of handing over an existing IP session, i.e., MN is requesting an independent IP session with the WiFi network without disrupting the IP session with the UTRAN/EUTRAN. In this case, no Session Id (Section 5.5) may be included.
- o 1 - MN intends to handover an existing IP session. In this case, MN may include a Session Id (Section 5.5) to correlate this WiFi session with a UTRAN/EUTRAN session.

## 5.5. AT\_HANOVER\_SESSION\_ID

When MN intends to handover an earlier IP session to the current access network, it may propagate identity that can help identify the previous session from UTRAN/EUTRAN that MN intends to handover. This attribute is defined as a generic octet string. MN may include EUTRAN GUTI if the previous session was a EUTRAN session. If the previous session was a UTRAN session, MN may include UTRAN Global RNC Id (MCC, MNC, RNC Id) and P-TMSI concatenated as an octet string.

This attribute can be included in any of the EAP Request message that are integrity protected, such as EAP-Response/AKA-Challenge.

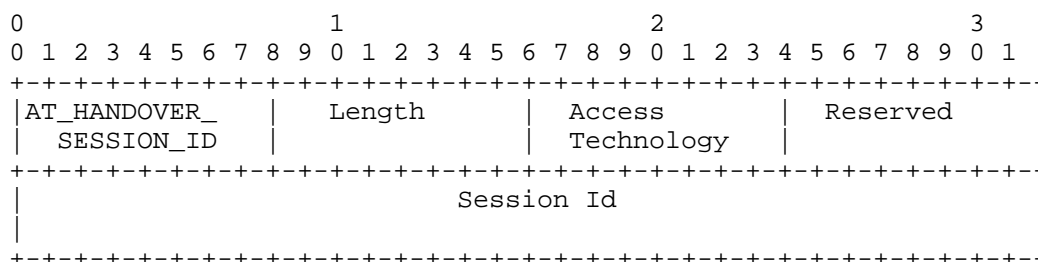


Figure 6: AT\_HANOVER\_SESSION\_ID EAP Attribute

## Access Technology:

This field represents the RAN technology from which the MN is undergoing a handover.

- o 0 - Reserved
- o 1 - UTRAN
- o 2 - EUTRAN

## Session Id:

An arbitrary octet string that identifies the session in the source access technology. As defined at the beginning of this section, the actual value is RAN technology dependent. For EUTRAN, the value is GUTI. For UTRAN, the value is Global RNC Id (6 bytes) followed by P-TMSI (4 bytes).

## 6. Security Considerations

This documents defines a new EAP attribute to extend the capability of EAP-AKA protocol as specified in Section 8.2 of RFC 4187 [RFC4187]. This attribute is passed from the MN to the AAA server.

The document does not specify any new messages or options to the EAP-AKA protocol.

## 7. IANA Considerations

This document defines four new non-skippable EAP attributes: the AT\_VIRTUAL\_NETWORK\_ID (TBD by IANA), AT\_VIRTUAL\_NETWORK\_REQ (TBD by IANA), AT\_HANDOVER\_INDICATION (TBD by IANA) and AT\_HANDOVER\_SESSION\_ID (TBD by IANA). All these attributes need IANA assignment.

## 8. Acknowledgment

Thanks to Sebastian Speicher for the review and suggesting improvements.

## 9. Informative References

- [3GPP-TS-33.402] "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses, 3GPP TS 33.402 8.6.0, December 2009.", , <<http://www.3gpp.org/ftp/Specs/html-info/33402.htm>>.
- [EPC] "General Packet Radio Service (GPRS);enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 8.8.0, December 2009.", , <<http://www.3gpp.org/ftp/Specs/html-info/23401.htm>>.
- [GPRS] "General Packet Radio Service (GPRS); Service description; Stage 2, 3GPP TS 23.060, December 2006", , <<http://www.3gpp.org/ftp/Specs/html-info/23060.htm>>.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC3748, June 2004, <<http://www.ietf.org/rfc/rfc3748.txt>>.
- [RFC4186] Haverinen, H. and J. Salowey, "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", RFC 4186, January 2006.
- [RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key

Agreement (EAP-AKA)", RFC4187, January 2006,  
<<http://tools.ietf.org/html/rfc4187>>.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC5415, January 2009,  
<<http://www.ietf.org/rfc/rfc5415.txt>>.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", RFC 5448, May 2009.

#### Appendix A. Change Log

- o: Initial Draft
- o: v01: status to Informational, Updated References, Revised the Figure
- o: No changes from 01 to 02
- o: Per recent 3GPP updates, added the Connectivity Type attribute to allow indicating Non-Seamless WLAN Offload or EPC connectivity
- o: version-04: Revised AT\_VIRTUAL\_NETWORK\_REQ to include 1) single PDN vs Multiple PDN connections, 2) PDN Types, and referred to NSW0 Connectivity Type attribute

#### Authors' Addresses

Ravi Valmikum  
Unaffiliated  
USA

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

Rajeev Koodli  
Cisco Systems  
USA

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



INTERNET-DRAFT  
Intended Status: Informational  
Expires: April 17, 2014

John Kaippallimalil  
Huawei  
Rajesh S. Pazhyannur  
Cisco  
Parviz Yegani  
Juniper  
October 14, 2013

Mapping Wi-Fi QoS in a PMIPv6 Mobility Domain  
draft-kaippallimalil-netext-pmip-qos-wifi-03

Abstract

This document provides a specification to enable end to end QoS in networks containing a Wi-Fi network coupled with a PMIPv6 mobility domain consisting of a local mobility anchor and mobility access gateway. This enables QoS policing and labeling of packets in a consistent manner on the 802.11 link between the MN and the AP as well as the link between the MAG and the LMA. To enable this, the document specifies mapping between QoS parameters on the 802.11 link and the QoS Mobility options in the PMIPv6 domain.

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) 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
1.1. Terminology . . . . .	3
1.2. Definitions . . . . .	4
1.3. Abbreviations . . . . .	4
2. Background . . . . .	4
2.1. QoS in 3GPP based Networks . . . . .	4
2.2. QoS in PMIPv6 Mobility domain . . . . .	5
2.3. QoS in IEEE 802.11 based Networks . . . . .	5
3. End-to-End QoS with Admission Control . . . . .	6
3.1. Case A: MN Initiated QoS Signaling . . . . .	6
3.2. Case B: Network Initiated QoS Signaling (802.11aa based) . . . . .	7
3.3. Case C: Hybrid (Network Initiated for PMIPv6 and MN initiated for Wi-Fi) . . . . .	9
3.4. Mapping of Connection Parameters . . . . .	10
3.5. Service Guarantees in 802.11 . . . . .	11
4. End-to-End QoS without Admission Control . . . . .	11
4.1. Default Values and Recommendations . . . . .	13
5. Security Considerations . . . . .	13
6. IANA Considerations . . . . .	13
7. References . . . . .	14
7.1. Normative References . . . . .	14
7.2. Informative References . . . . .	14
Authors' Addresses . . . . .	15
Appendix A: QoS Policy Architecture . . . . .	16

## 1. Introduction

The deployment network considered here is where there is a Wi-Fi access link coupled with a PMIPv6 mobility domain. A MAG is co-located with the Access Point (AP) and in cases where the Wi-Fi network consists of Access Point and a Wireless LAN Controller (WLC), we assume that the MAG is located either at the AP or the WLC. Additionally, the Wi-Fi access network may be part of a 3GPP network. In such a case, the per user QoS Policy may be provided from the 3GPP network. Specifically, the 3GPP network may provision QoS during authorization of the user, and may also dynamically provision QoS for individual flows. [TS23.402] [TS23.273] describe the initial authorization and download of user profile, including QoS profile. In this specification we describe how end to end QoS may be established: spanning the access domain (Wi-Fi access network) and the PMIPv6 mobility domain between the MAG and the LMA. A key question from an end to end QoS standpoint is how QoS policies on the Wi-Fi access link is mapped to QoS in the PMIPv6 mobility domain and further to 3GPP QoS policies for per user/per flow.

[PMIP-QoS] defines a QoS option to enable QoS in the PMIPv6 mobility domain. The sub-options defined in the QoS option are mapped into corresponding parameters in the 3GPP specified QoS parameters. [PMIP-QoS] does not explicitly describe how the QoS signaling and QoS sub-options map into corresponding signaling and parameters in the Wi-Fi access network. This mapping is the focus of this document. The key distinction between [PMIP-QoS] and this document is that this focuses on the end-to-end flow (spanning 802.11 access and PMIPv6 domain) while [PMIP-QoS] focuses on the QoS within the PMIPv6 mobility domain. This document provides a systematic way to map to 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, 3GPP and 802.11.

The rest of the document is organized as follows. Chapter 2 provides an overview of the QoS mechanisms in 3GPP mobile networks and 802.11 networks. Chapter 3 describes different ways how end to end QoS with Wi-Fi admission control is achieved. Chapter 4 describes how end to end QoS without admission control is achieved.

### 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 3GPP mobile network defines the guaranteed (reserved) bit rate resources of service data flow on a connection (bearer) [TS23.203].

### Aggregate Maximum Bit Rate (AMBR)

AMBR represents the total bandwidth that all flows of a user is allowed.

### 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].

### Mean Data Rate

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

## 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
PDN-GW	Packet Data Network Gateway
QCI	QoS Class Indicator
QoS	Quality of Service
Tspec	Traffic Conditioning Spec
WLC	Wireless Controller

## 2. Background

### 2.1. QoS in 3GPP based 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].

In a 3GPP radio network, priority and packet delay budget in QCI determines the policy used for rate-shaping, scheduling and queue management. The ARP is used to determine if a connection session request should be allowed (e.g. insufficient radio resource) and the order in which flows should be pre-empted in case of severe congestion.

An MN may have more than one IP addresses associated with the same hardware (MAC) address corresponding to each of the networks than it is attached to. This corresponds to more than one PMIP mobility session for which QoS is provisioned in the WLC.

## 2.2. 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 a subscriber's IP flows. Using the QoS option, the local mobility anchor and the mobile access gateway can exchange available QoS attributes and associated values. This enables QoS policing and labeling of packets to enforce QoS differentiation on the path between the local mobility anchor and the mobile access gateway.

## 2.3. QoS in IEEE 802.11 based Networks

IEEE 802.11-2012 [802.11-2012] provides an enhancement of the MAC layer in WiFi networks to support QoS--EDCA (Enhanced Distributed Channel Access). EDCA uses a contention based channel access method.

The EDCA mechanism provides 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.

In addition to the above, QoS can also be provided using admission control. The MN uses ADDTS (Add Traffic Specs) to setup 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.

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

This section outlines a few use cases to illustrate how the parameters and mapping in section 4 are applied. These cases are not expected to be exhaustive.

There are two main types of interaction possible to provision QoS - one is where the UE 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 this scenario, if the MN supports 802.11aa (TCLAS), the network can push the QoS configuration to the MN. If the MN only supports WMM QoS, then MN requests for QoS for the WiFi segment and the MAG provisions based on QoS already provisioned for the MN.

#### 3.1. Case A: MN Initiated QoS Signaling

When an MN sets up a connection that requires admission control in the WiFi network, the level of QoS for the connection needs to be set up. When the MN is configured (e.g. in SIM, subscription) to start the QoS signaling, it sends an ADDTS request indicating the QoS required for the connection. The AP/WLC (MAG) obtains the corresponding level of QoS to be granted to the flow by sending a PMIPv6 PBU message with QoS options to the LMA. Details of the setup are described below.

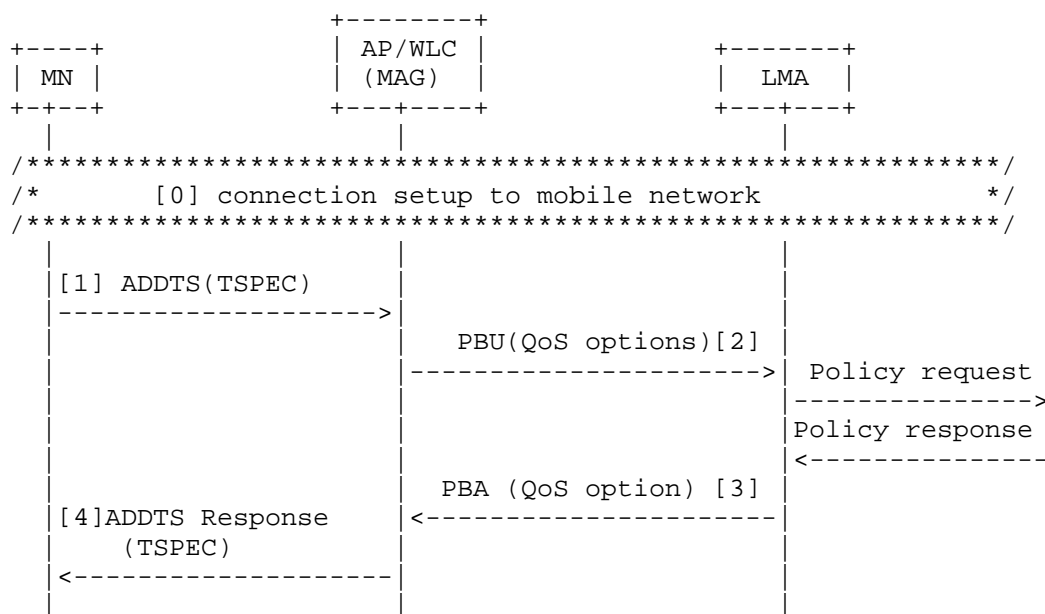


Figure 1: MN initiated QoS setup

- [0] The MN starts signaling to setup the connection. In mobile networks, these are not default connections that are setup initially. Default connections are best effort and do not need explicit admission control with ADDTS.
- [1] If the MN and network support 802.11aa and the MN is configured to start QoS signaling, the MN sends an ADDTS request specifying the QoS requested for the traffic stream including TSPEC element with connection setup identifier.
- [2] The MAG (AP/WLC) identifies the PMIP based on the connection identifier and sends a PBU with QoS options requested.
- [3] The LMA responds with the authorized QoS for the connection.
- [4] The AP/WLC (MAG) provisions the corresponding QoS and replies with ADDTS Response containing authorized QoS in TSPEC.

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

When an MN has connections or flows that require admission control, the mobile network may provision correspond QoS in the MAG. This use case illustrates how an MN and WiFi network that supports 802.11aa

can provision QoS to the MN. In this case, the network is configured to start the QoS signaling, it sends an ADDTS request indicating the QoS required for the connection.

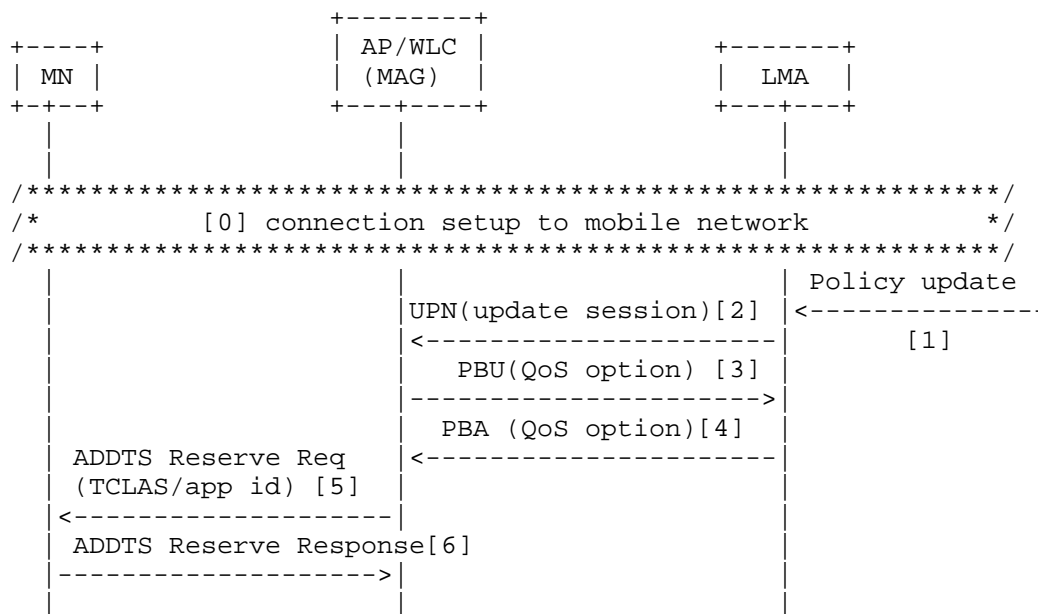


Figure 2: Network initiated QoS setup with 802.11aa

- [0] The MN starts signaling to setup the connection. In mobile networks, these are not default connections that are setup initially. Default connections are best effort and do not need explicit admission control with ADDTS.
- [1] The LMA gets a QoS policy update for an existing connection.
- [2] LMA sends a PMIP UPN (Update Notification) message to the MAG requesting it to update session parameters.
- [3] The MAG (AP/WLC) replies to UPN with a PBU including QoS options.
- [4] The LMA responds with the authorized QoS for the connection.
- [5] If the MN and network support 802.11aa, the AP/WLC (MAG) sends an ADDTS Reserve Request specifying the QoS reserved for the traffic stream including TSPEC and TCLAS element with the connection identifier (from PMIP).

- [6] The MN notes the QoS reserved in the network and replies with ADDTS Reserve Response.

### 3.3. Case C: Hybrid (Network Initiated for PMIPv6 and MN initiated for Wi-Fi)

This example outlines a scenario where an MN attaches to the WiFi 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.

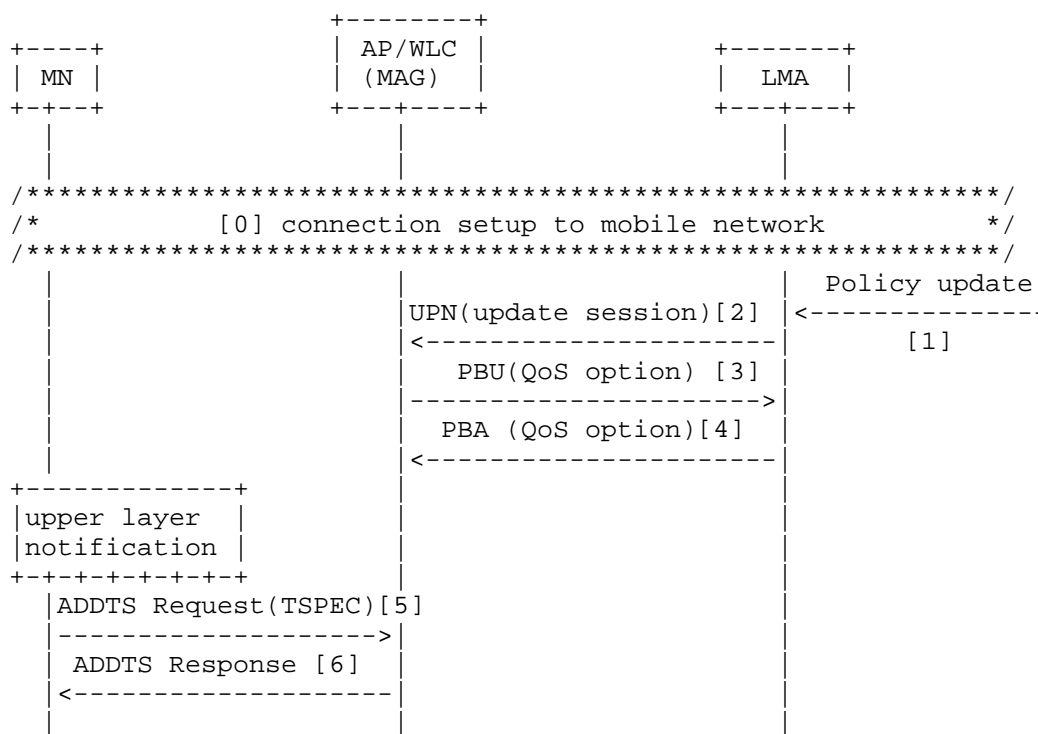


Figure 3: Network initiated QoS setup with WMM

- [0] The MN starts signaling to setup the connection. In mobile networks, these are not default connections that are setup initially. Default connections are best effort and do not need explicit admission control with ADDTS.

- [1] The LMA gets a QoS policy update for an existing connection.
- [2] LMA sends a PMIP UPN (Update Notification) message to the MAG requesting it to update session parameters.
- [3] The MAG (AP/WLC) replies to UPN with a PBU including QoS options.
- [4] The LMA responds with the authorized QoS for the connection. Since the MAG or MN does not support 802.11aa, the MAG updates QoS profile of MN and waits for request from MN.
- [5] When the MN receives upper layer signaling (e.g. SDP) indicating acceptance of codec or other media parameters, the MN requests for corresponding QoS in TSPEC of ADDTS Request.
- [6] When the (AP/WLC (MAG) receives the ADDTS Request from MN, it checks the QoS profile for the MN to see if the additional QoS requested for the stream is consistent with the QoS profile stored for the MN. The AP/WLC then responds with ADDTS Response.

### 3.4. Mapping of Connection Parameters

This section outlines the handling of QoS connection (session) parameters between WiFi 802.11 and PMIP QoS.

#### Connection Mapping:

802.11 QoS in TSPEC is used to reserve QoS for a traffic stream (MN MAC, TS(Traffic Stream) id). The QoS reservation is for 802.11 frames and here is no IP prefix/flow associated during this reservation. The AP/WLC evaluates this request against policy installed using PMIP QoS. When PMIP QoS policy is installed in AP/WLC, the TSPEC request is granted if the MN (identified by MAC) is authorized. The AP/WLC may police subsequent flows with {MAC, TS, 802.1D, IP prefix} to match QoS policy installed by PMIP QoS for {IP prefix, DSCP}.

#### QoS Class:

802.11 QoS Access Class (AC\_VO, AC\_VI) requests corresponds to DSCP in PMIP QoS setup. Table 1 (section 4.1) below shows the complete mapping.

#### Bandwidth:

For flows with reservation, the 802.11 Mean Data Rate should be

equal to (or less than) Guaranteed Bit Rate (GBR). If the MN requests Mean Data Rate in ADDTS greater than GBR, then AP/WLC should deny the request in ADDTS Response.

For flows with no reservation, the bandwidth should not exceed MBR (Maximum Bit Rate). If such a flow is offloaded at AP/WLC, the policy obtained during authorization is used.

The total bandwidth used by all flows of an MN should not exceed AMBR (Aggregate Maximum Bit Rate).

#### Preemption Priority:

Mobile networks configure ARP (Allocation Retention Priority) during authorization and in [PMIPv6 QoS]. If there is limited resource and multiple ADDTS requests, ARP should be used by the AP/WLC to determine which requests to grant. ARP has a range 1 to 15 with 1 being the highest priority [TS23.203].

During severe congestion or partial failure, if the AP/WLC has to preempt existing reservations, ARP may be used to determine the order of preemption.

### 3.5. 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 WiFi 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 WiFi 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 WiFi 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. End-to-End QoS without Admission Control

GSMA and IETF (RFC 4594) have defined mapping between DSCP and IEEE 802.11 UP (user Priority). The MAG could be pre-configured to use the mapping from one of these specifications. Per MN connection configuration may be setup at the AP/WLC based by PMIP QoS signaling during connection setup. This is described in [PMIP QoS], section 3.5.

However, in many cases it may be beneficial to use a different set of mapping and potentially different mappings for different users. For example an operator may choose to provide only best effort service to one subscriber class while providing more enhanced (AF or EF) services to other subscriber classes. To enable such capabilities, a QoS Service Attribute called QoS MAP Set is introduced. This is modeled after an IEEE 802.11 element with the same name (see 8.4.2.97 in IEEE 802.11-2012).

The QoS Map Set attribute is used as follows. The LMA would send a specific DSCP to UP mapping in the Proxy Binding Update. In cases where the MAG is co-located with the AP, AP/MAG can ensure that received packets from the mobile node have the the correct DSCP to UP mapping (packets with inappropriate marking may be remarked). Similarly, on the downstream, the QoS Map Set enables the MAG/AP to determine the correct UP. This also ensures that a source ineligible for higher grades of service (provided by higher priority UP bits) cannot avail of such a service by marking the packets with DSCP values (for example by marking the packets with EF and AF codepoints). There is an additional benefit of providing the AP/MAG with the QoS Map Set. For mobile nodes that support the IEEE 802.11 QoS Map Set capability, the AP can provide the corresponding QoS Map Set information to the mobile node. This can ensure that the mobile node uses the correct DSCP to UP marking.

0								1								2								3							
0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
Type																															
UP0 Range								UP1 Range								UP2 Range								UP3 Range							
UP4 Range								UP5 Range								UP6 Range								UP7 Range							
DSCP Ex-0								DSCP Ex-1								DSCP Ex-3 ....															

Type: TBD Length: Length of the following data value in octets, greater than or equal to 10.

The format of UP0,...,UP7 Range is as follows

```

      0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
    +=+--+--+--++=+--+--+--+--+--+--+
    | DSCP Low Val | DSCP Hi Val |
    +=+--+--+--++=+--+--+--+--+--+

```

The format of the DSCP Exception field is as follows

```

      0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7
    +=+--+--+--++=+--+--+--+--+--+--+
    | DSCP Val      |      UP Value  |
    +=+--+--+--++=+--+--+--+--+--+

```

#### 4.1. Default Values and Recommendations

The table below outlines a recommended mapping between 3GPP QCI, and 802.11 Access Category (AC)/ 802.1D UP.

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	IMS 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 1: QoS Mapping between QCI/DSCP, 802.1D UP, WMM AC

The QoS mapping table above provides recommendations and default mapping between DSCP provided in [PMIP QoS], WMM AC used for TSPEC reservation, and 802.1D UP in 802.11 frames.

#### 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-00, June 2012.
- [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 Policy Architecture

The QoS architecture in this section provides a brief outline for provisioning QoS in a consistent manner across the WiFi network, backhaul and PMIP mobile network.

QoS information is available to AP/WLC when the MN attaches to the WiFi network and authenticates. The authorization profile includes QoS that the user/MN has subscribed to. When the MN attaches to the network, the LMA returns the session parameters such as IP address and may also include QoS profile as per [PMIP-QoS].

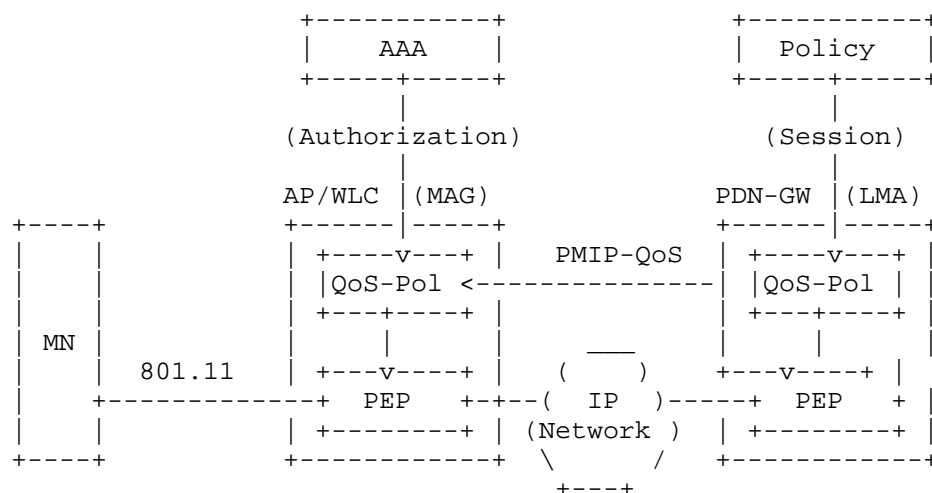


Figure 4: Architecture for provisioning QoS Policy on WiFi AP

Figure 4 provides an overview of the architecture in which QoS for an MN is provisioned on the AP/WLC. MN QoS policy from initial authorization and PMIP connection establishment is provisioned in the AP/WLC QoS-Pol (logical function). AP/WLC PEP uses the policies for handling QoS flows from an MN.

Policy Server provisioning of Admission control for connections has traditionally relied on information from Deep Packet Inspection (DPI) or Application Level Gateways (ALG). DPIs and ALGs cannot however determine the MNs subscribed bandwidth or QoS. The alternative is to provision QoS policy for a user's connections and use subscribed policy and PMIP QoS policy. When the AP/WLC has both the subscribed QoS policy and policy parameters from PMIP QoS, the QoS parameters obtained through PMIP reflect the policy that accounts for current network conditions.

In mobile networks, default connections are not setup with a bandwidth reservation and hence do not have a GBR (Guaranteed Bit Rate) associated. However, the PDN-GW (LMA) polices the AMBR (Aggregate Maximum Bandwidth Rate) - the maximum bit rate for all flows to/from the MN. Thus, upstream traffic should be policed by AP/WLC to not exceed the maximum prescribed in AMBR values. The AP/WLC should also schedule traffic for these connections as background or best effort (AC\_BK, AC\_BE) and the corresponding 802.1D

For voice, video and other applications that require reservation of QoS resources, a dedicated PMIP connection is setup in mobile networks and the PDN-GW (LMA) reserves resources as per GBR (Guaranteed Bit Rate) for upstream and downstream. In this also, the total bit rate of all flows to/from MN should not exceed the maximum bit rates in AMBR (Aggregate Maximum Bit Rate). Upstream and downstream traffic should be scheduled by MN and AP/WLC using ADDTS (TSPEC) for voice or video (AC\_VO, AC\_VI). The MN should also include the Mean Data Rate for the connection based on the requirements of the application or negotiated codec. The AP/WLC grants resources based on policy obtained over PMIP QoS. GBR values in PMIP QoS should be used to derive Mean Data Rate as described in section 4.1. When the MN completes the session, it may send DELTS to request release of associated QoS resources.

If the MN connection is offloaded to the internet by the AP/WLC, there is no corresponding PMIP session setup to the mobile network. In this case, the AP/WLC may use AMBR obtained during authorization if the MN has no other connections to the mobile network. If the MN has other connections to the mobile network, the AP/WLC should limit the maximum bit rate of all flows of the MN to AMBR obtained in PMIP QoS.

When the network is congested and the AP/WLC cannot grant the QoS requested by MN, the AP/WLC should refuse the ADDTS request and not continue the PMIP QoS signaling request. The application in MN may downgrade the codec and re-negotiate a new TSPEC/resource request that the AP/WLC may grant. If the AP/WLC cannot handle committed

connections due to network degradation or other partial failures, the AP/WLC may use the ARP (Allocation Retention Priority) values of the connection to gracefully release resources.

NETEXT WG  
Internet-Draft  
Intended status: Standards Track  
Expires: April 25, 2014

R. Pazhyannur  
S. Speicher  
S. Gundavelli  
Cisco  
J. Korhonen  
Broadcom  
October 22, 2013

Civic Location ANI Suboption for PMIPv6  
draft-pazhyannur-netext-civic-location-ani-subopt-00.txt

## Abstract

This specification extends the Access Network Identifier mobility option for carrying the Civic Location information of the mobile node from the mobile access gateway to the local mobility anchor. This specification also 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 the freshness of the ANI.

## 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 25, 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 . . . . .	2
2. Conventions and Terminology . . . . .	4
2.1. Conventions . . . . .	4
2.2. Terminology . . . . .	4
3. Civic Location Sub-Option . . . . .	4
4. ANI Update-Frequency Sub-Option . . . . .	5
5. Usage Example . . . . .	5
6. IANA Considerations . . . . .	6
7. Security Considerations . . . . .	7
8. Acknowledgements . . . . .	7
9. References . . . . .	7
9.1. Normative References . . . . .	7
9.2. Informative References . . . . .	8
Authors' Addresses . . . . .	8

## 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 or in some cases provide access network identifiers to other systems like location based applications. RFC 6757 defined new mobility options to enable a MAG to provide such information. When this used in Wi-Fi systems the Access Network Identifier could carry the identifier of the Access Point (for instance the BSSID or the geo-spatial coordinates of the Access Point). For example, when a client associates with an Access Point in a Wi-Fi hotspot, the MAG would send the ANI information (like SSID, BSSID, geo-location) to the LMA. In many indoor AP deployments, it may be difficult to provide Geo-spatial coordinates of APs but for many location based applications, the civic location may be sufficient. [RFC4776] provides further motivations on usage of civic information in providing human-usable information, particularly within buildings. To provide civic location information, this document defines a new ANI sub-option.

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. This PBU would contain ANI information corresponding to the target Access Point. As a result, the LMA has the current ANI. For example, if the MAG sent BSSID or geo-location, then the LMA would have the latest information about the client's 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 Access Point to another. 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. This is because, the LMA will only have the ANI information at the time of the PBU, but the ANI may have changed due to handovers within the access network (which are not visible to LMA).

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 would be 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. In these deployments the mobility within the venue is not handled by PMIPv6 but handled by some layer 2 mechanism, while the mobility across venues is provided by PMIPv6. If MAG sends PBU with every intra-venue handover, this may result in a large number of PMIPv6 transactions on the transactions in the MAG and LMA. Moreover, since mobility inside the LMA may not be handled by PMIPv6, these transactions are being sent only to update the ANI. This document describes a method to solve this problem.

This specification extensions to Access Network Identifier mobility option for carrying the Civic 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 information 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 [RFC6463]. This sub-option carries the Civic Location information of the mobile node as known to the mobile access gateway. There MUST be no more than a single instance of this specific sub-option in any Access Network Identifier option. The format of this option is defined below.

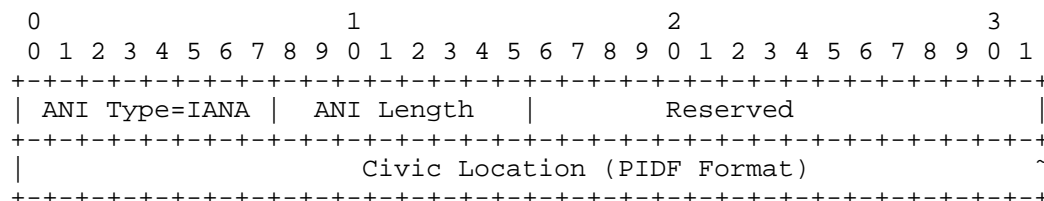


Figure 1: Network-Identifier Sub-option

**ANI Type:** It MUST be set to value of (1), indicating that its a Network-Identifier sub-option

**ANI Length:** Total length of this sub option in octets, excluding the ANI Type and ANI length fields. The value can be in the range of 5 to 32 octets.

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

**Civic Location:** This format is as specified in the Presence Information Data Format Location Object [RFC5139].

#### 4. ANI Update-Frequency Sub-Option

The ANI Update Frequency is a mobility sub-option carried in the Access Network Identifier option defined in [RFC6463]. This option gives a hint regarding for how long the ANI information should be considered current. This applies to all the ANI sub-options present in the ANI option. (If there is a need to specify different Time-To-Live values for different ANI sub options, then the MAG may provide multiple ANI options each with its corresponding Time-To-Live value. This may be motivated by the fact that certain ANI sub-options such as Network Identifier sub-option may have longer Time-To-Live values compared to Geo-Location sub-otion. The data type of this field is a string and the content is expressed in the 64-bit Network Time Protocol (NTP) timestamp format [RFC1305].

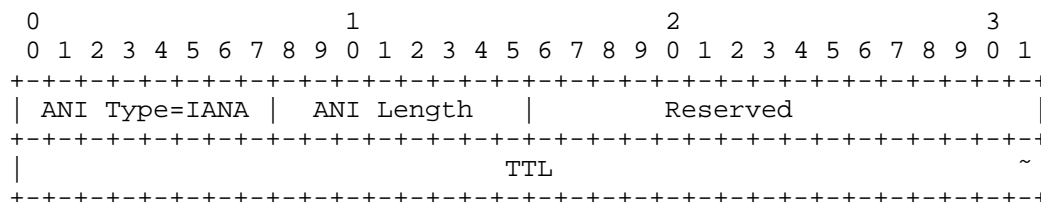


Figure 2: Network-Identifier Sub-option

**ANI Type:** It MUST be set to value of (1), indicating that its a Network-Identifier sub-option

**ANI Length:** Total length of this sub option in octets, excluding the ANI Type and ANI length fields. The value can be in the range of 5 to 32 octets.

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

**TTL:** TTL Format - TBD

#### 5. 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 a Time-to-Live ANI sub option

- o Application request LMA for ANI Information
- o if ANI information is current 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

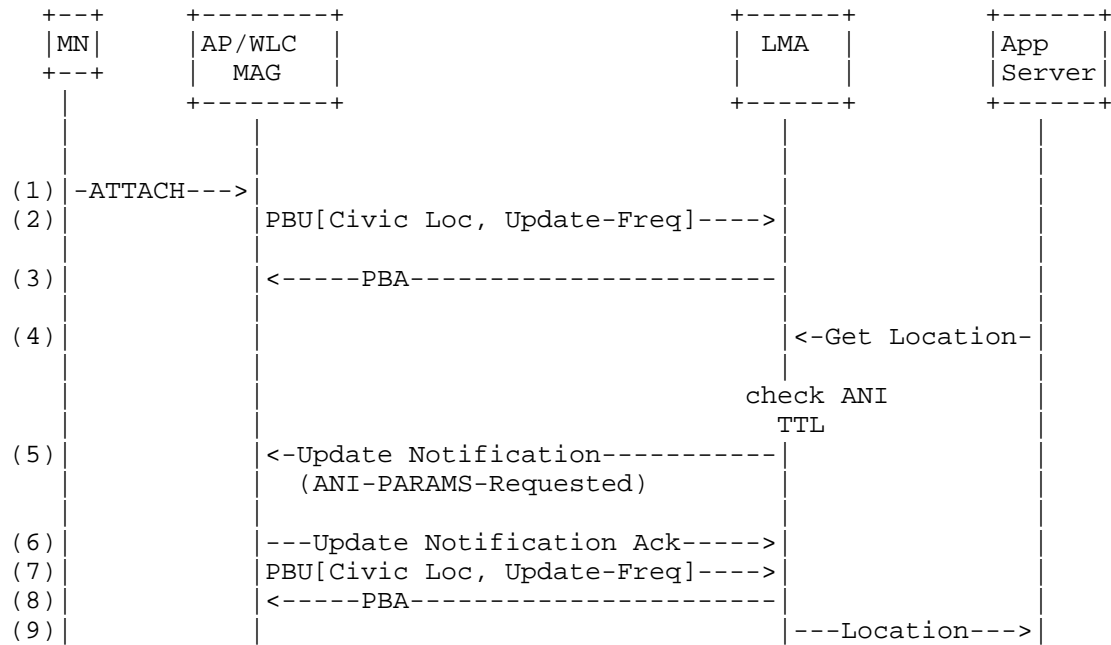


Figure 3: Usage Example

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

## 6. 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 ANI-Update-Frequency 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.

## 7. 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 [RFC6463]. 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 [RFC6463]. Therefore, it inherits from [RFC5213] and [RFC6463], its security guidelines and does not require any additional security considerations.

## 8. Acknowledgements

TBD

## 9. References

### 9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [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.

## 9.2. 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.
- [RFC6463] Korhonen, J., Gundavelli, S., Yokota, H., and X. Cui, "Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6", RFC 6463, February 2012.

## Authors' Addresses

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

Email: rpazhyan@cisco.com

Sebastian Speicher  
Cisco  
Richtistrasse 7  
Wallisellen, Zurich 8304  
Switzerland

Email: sespeich@cisco.com

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

Email: sgundave@cisco.com

Jouni Korhonen  
Broadcom  
Porkkalankatu 24  
Helsinki FIN-00180  
Finland

Email: jouni.nospam@gmail.com