

NETEXT WG
Internet-Draft
Intended status: Standards Track
Expires: January 16, 2014

M. Liebsch
NEC
P. Seite
Orange
H. Yokota
KDDI Lab
J. Korhonen
Renesas Mobile
S. Gundavelli
Cisco
July 15, 2013

Quality of Service Option for Proxy Mobile IPv6
draft-ietf-netext-pmip6-qos-03.txt

Abstract

This specification defines a new 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. Furthermore, making QoS parameters available on the MAG enables mapping these parameters to QoS rules being specific to the access technology which operates below the mobile access gateway. After such mapping, QoS rules can be enforced on the access technology components, such as an IEEE 802.11e Wireless LAN controller.

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 January 16, 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	5
2. Conventions and Terminology	7
2.1. Conventions	7
2.2. Terminology	7
3. Description of the Technical Approach	8
3.1. Technical Scope and Procedure	8
3.2. Use Case A -- Handover of Available QoS Context	9
3.3. Use Case B -- Establishment of new QoS Context in non-cellular Access	10
3.4. Use Case C -- Dynamic Update to QoS Policy	11
3.5. Relevant QoS Attributes	12
3.6. Protocol Operation	13
3.6.1. Handover of existing QoS rules	14
3.6.2. Establishment of QoS rules	15
4. Protocol Considerations	16
4.1. Mobile Access Gateway Considerations	16
4.2. Local Mobility Anchor Considerations	17
5. Quality of Service Option	18
6. Format of the Quality of Service Attribute	19
6.1. Per Mobile Node Aggregate Maximum Downlink Bit Rate	19
6.2. Per Mobile Node Aggregate Maximum Uplink Bit Rate	20
6.3. Per Mobility Session Aggregate Maximum Downlink Bit Rate	20
6.4. Per Mobility Session Aggregate Maximum Uplink Bit Rate	21
6.5. Allocation and Retention Priority	21
6.6. Guaranteed Downlink Bit Rate	23
6.7. Guaranteed Uplink Bit Rate	23
6.8. Traffic Selector	24
7. IANA Considerations	25
8. Security Considerations	26
9. Acknowledgements	27
10. References	28
10.1. Normative References	28
10.2. Informative References	28
Appendix A. Information when implementing PMIP based QoS support with IEEE 802.11e	30

Appendix B. Information when implementing with a Broadband
Network Gateway 34

Authors' Addresses 35

1. Introduction

Mobile operators deploy Proxy Mobile IPv6 (PMIPv6) [RFC5213] to enable network-based mobility management for mobile nodes (MN). Users can access Internet Protocol (IP) based services from their mobile device by using different radio access technologies. Current standardization effort considers strong QoS classification and enforcement for cellular radio access technologies. QoS policies are typically controlled by a policy control function, whereas the policies are enforced by different gateways in the infrastructure, such as the LMA and the MAG, as well as by access network elements. Policy control and QoS differentiation for access to the mobile operator network through alternative non-cellular access technologies is not yet considered, even though some of these access technologies are able to support QoS by appropriate traffic prioritization techniques. However, handover and IP Flow Mobility using alternative radio access technologies, such as IEEE802.16 and Wireless LAN according to the IEEE802.11 specification, are being considered by the standards [TS23.402], whereas inter-working with the cellular architecture to establish QoS policies in alternative access networks has not been focussed on so far.

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

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

This document specifies an extension to the PMIPv6 protocol to establish QoS policies for an MN's data traffic on the LMA and the MAG. QoS policies are conveyed in-band with PMIPv6 signaling using the specified QoS option and are enforced on the LMA for downlink traffic and on the MAG for uplink traffic. The specified option allows association between IP session classification characteristics, such as a Differentiated Services Code Point (DSCP), and the expected QoS class for this IP session. This document specifies fundamental

QoS attributes which apply per Mobile Node, others that apply per Mobility Session. Additional attributes are specified, which can identify if they apply either per Mobility Session or per flow. Further handling of QoS policies between the MAG and the WLAN Controller (WLC) or WLAN Access Point is out of scope of this specification.

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 the Proxy Mobile IPv6 specifications [RFC5213], [RFC5844], [RFC5845] and [RFC5846]. Additionally, this document uses the following abbreviations:

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

3. Description of the Technical Approach

3.1. Technical Scope and Procedure

The QoS option specified in this document supports the setup of states on the LMA and the MAG to allow enforcement of QoS policies for packet differentiation on the network path between the LMA and the MAG providing non-cellular access to the mobile operator network. QoS differentiation is typically enabled in the mobile operator's network using Differentiated Services techniques in the IP transport network, whereas radio access specific QoS differentiation depends on the radio technology in use. Whereas very accurate and fine granular traffic classes are specified for the cellular radio access, the IP transport network only supports enforcement of few Differentiated Services classes according to well-known Differentiated Services Code Points (DSCP) [GSMA.IR.34].

Central control from a Policy Control Function (PCF) is deployed in current cellular mobile communication standards to assign an appropriate QoS class to an MN's individual flows. Non-cellular access technologies are not yet considered for per-flow QoS policing under control of a common PCF. The QoS option specified in this document enables exchange of QoS policies, which have been setup for an MN's IP flows on the cellular network, between the LMA and a new MAG during handover from the cellular access network to the non-cellular access network. Furthermore, the QoS option can be used to exchange QoS policies for new IP flows, which are initiated while the MN is attached to the non-cellular MAG.

Figure 1 illustrates a generalized architecture where the QoS option can be used. During an MN's handover from cellular access to non-cellular access, e.g. a wireless LAN (WLAN) radio access network, the MN's QoS policy rules, as previously established on the LMA for the MN's communication through the cellular access network, are moved to the handover target MAG serving the non-cellular access network. Such non-cellular MAG can have an access technology specific controller or function co-located, e.g. a Wireless LAN Controller (WLC), as depicted in option (I) of Figure 1. Alternatively, the access specific architecture can be distributed and the access technology specific control function is not co-located with the MAG, as depicted in option (II). In case of a distributed access network architecture as per option (II), the MAG and the access technology specific control function (e.g. the WLC) must provide some protocol for QoS inter-working. Details of such inter-working are out of scope of this specification.

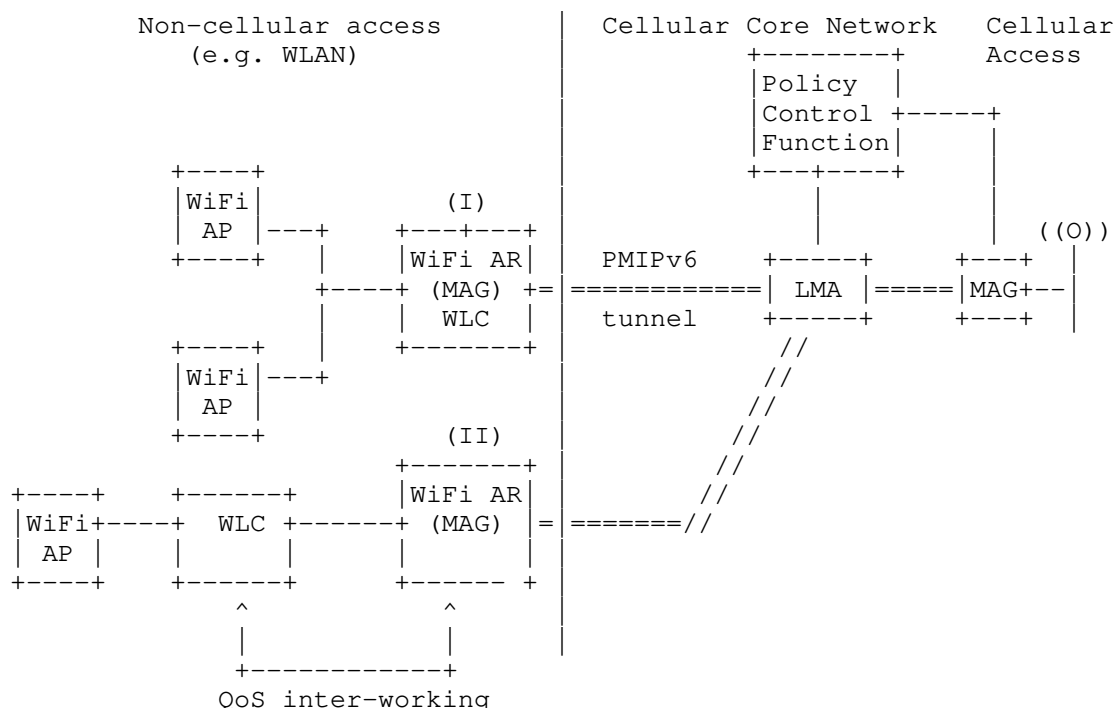


Figure 1: Architecture for QoS inter-working between cellular access and non-cellular access

Based on the architecture illustrated in Figure 1, two key use cases can be supported by the QoS option. Use case A assumes a MN is attached to the network through cellular access and its LMA has QoS policy rules for the MN's data flows available. This specification does not depend on the approach how the cellular specific QoS policies have been configured on the LMA. During its handover, the available QoS policies are established on the handover target MAG, which serves the non-cellular access network. Use case B assumes that new policies need to be established for a MN as a new IP flow is initiated while the MN is attached to the network through the non-cellular network. These use cases are described in more detail in the subsequent sections Section 3.2 and Section 3.3 respectively.

3.2. Use Case A -- Handover of Available QoS Context

The MN is first connected to the cellular network, e.g. an LTE network, and having a multimedia session such as a video call with appropriate QoS parameters set by the policy control function. Then, the MN discovers a WiFi AP (e.g., at home or in a cafe) and switches to it provided that WiFi access has a higher priority when available.

Not only is the session continued, but also the QoS is maintained after moving to the WiFi access. In order for that to happen, the LMA delivers the QoS parameters to the MAG on the WLC via the PMIPv6 signaling and the equivalent QoS treatment is provided toward the MN on the WiFi link.

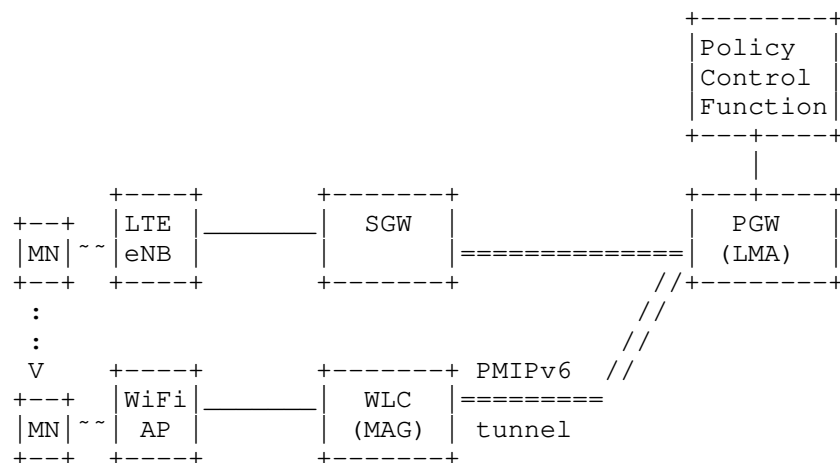


Figure 2: Handover Scenario

3.3. Use Case B -- Establishment of new QoS Context in non-cellular Access

A single operator has deployed both a fixed access network and a mobile access network. In this scenario, the operator may wish a harmonized QoS management on both accesses. However the fixed access network does not implement a QoS control framework. So, the operator chooses to rely on the 3GPP policy control function, which is a standard framework to provide a QoS control, and to enforce the 3GPP QoS policy to the Wi-Fi Access network. The PMIP interface is used to realize this QoS policy provisioning.

The use-case is depicted on Figure 3. The MN is first attaching to the Wi-Fi network. During attachment process, the LMA, which may be in communication with Policy Control Function (this step of the process is out of the scope of this document), provides the QoS parameters to the MAG piggy-backing the PMIP signaling (i.e. PBA). Subsequently, an application on the MN may trigger the request for enhanced QoS resources, e.g., by use of the WMM-API [80211e]. The MN

may request traffic resources be reserved using L2 signalling, e.g., sending an ADDTS message [80211e]. The request is relayed to the MAG which piggybacks the QoS parameters on the PMIP signalling (i.e. PBU initiated on the flow creation). The LMA, in co-ordination with the PCF, can then authorize the enforcement of such QoS policy. Then, the QoS parameters are provided to the MAG piggy-backing the PMIP signaling and the equivalent QoS treatment is provided towards the MN on the WiFi link.

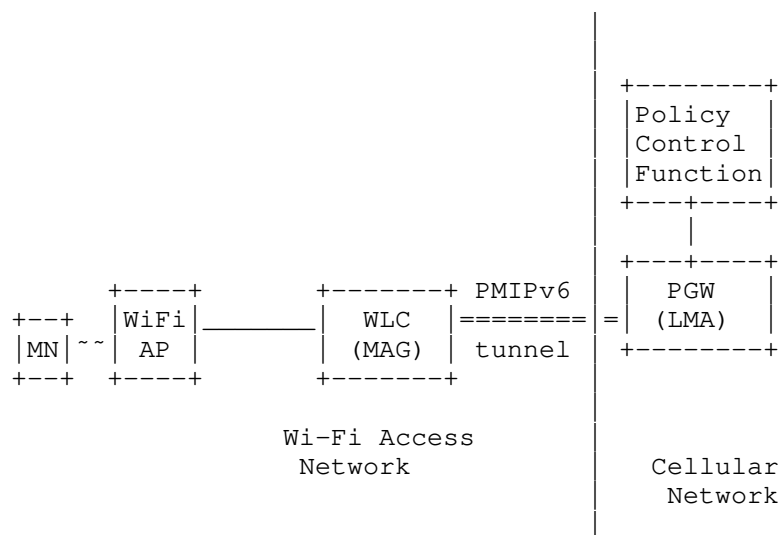


Figure 3: QoS policy provisioning

3.4. Use Case C -- Dynamic Update to QoS Policy

A mobile node is attached to the WLAN access and has obtained QoS parameters from the LMA for that mobility session. Having obtained the QoS parameters, a new application, e.g. IMS application, gets launched on the mobile node that requires certain QoS support.

The application on the mobile node initiates the communications via a dedicated network function (e.g. IMS Call Session Control Function). Once the communication is established, the application network function notifies the PCRF function about the new IP flow. The PCRF function in turn notifies the LMA about the needed QoS parameters identifying the IP flow and QoS parameters. LMA sends a Update Notification message [I-D.ietf-netext-update-notifications] to the MAG with the "Notification Reason" value set to "Force REREGISTER".

The MAG, on receiving the Update Notification message, completes the PBU/PBA signaling for obtaining the new QoS parameters. MAG provisions the newly obtained QoS parameters on the access network to ensure the newly established IP flow gets some dedicated network resources. Upon termination of the new flow, the application network function again notifies the PCRF function for removing the established bearers. The PCRF notifies the LMA for withdrawing the QoS resources establishes for that voice flow. LMA sends a Update Notification message to the MAG with the "Notification Reason" value set to "Force REREGISTER". MAG on receiving this message UpdateNotification Ack and completes the PBU/PBA signaling for obtaining the new QoS parameters. MAG provisions the newly obtained QoS parameters on the access network to ensure the dedicated network resources are now removed.

3.5. Relevant QoS Attributes

The QoS Option shall at least contain a DSCP value being associated with IP flows of a mobility session. Optional QoS information could also be added. For instance, in order to comply with 3GPP networks QoS, at minimum there is a need to convey the following additional QoS parameters for each PMIPv6 mobility session:

1. Per Mobile Node Aggregate Maximum Bit Rate (MN-AMBR) to both uplink and downlink directions.
2. Per mobility session Aggregate Maximum Bit Rate (MS-AMBR) to both uplink and downlink directions.

The following attributes represent a useful set of QoS parameters to negotiate during the session setup:

1. Allocation and Retention Priority (ARP).
2. Guaranteed Bit Rate (GBR)
3. Maximum Bit Rate (MBR)

For some optional QoS attributes the signaling can differentiate enforcement per mobility session and per IP flow. For the latter, the rule associated with the identified flow(s) overrule the aggregated rules which apply per Mobile Node or per Mobility Session. Additional attributes can be appended to the QoS option, but their definition and specification is out of scope of this document and left to their actual deployment.

Informational Note: If DSCP values follow the 3GPP specification and deployment, the code point can carry intrinsically additional

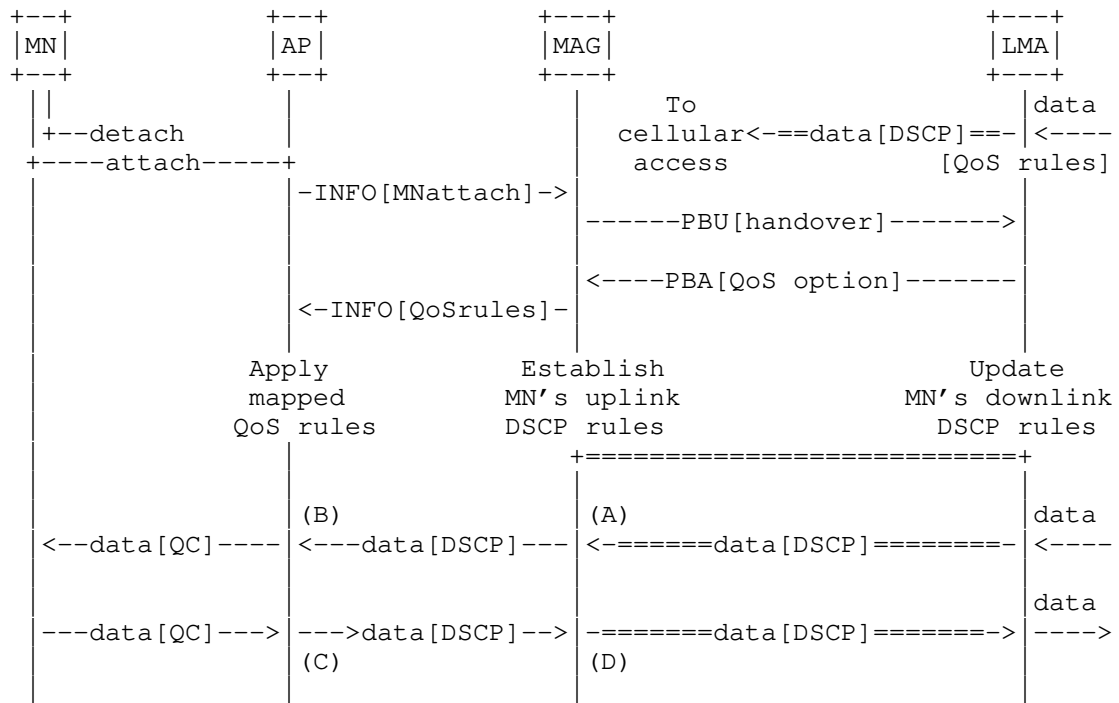
attributes according to a pre-defined mapping table:

This is the GSMA/3GPP mapping for EPC/LTE:

QCI	Traffic Class	DiffServ PHB	DSCP
1	Conversational	EF	101110
2	Conversational	EF	101110
3	Conversational	EF	101110
4	Streaming	AF41	100010
5	Interactive	AF31	011010
6	Interactive	AF32	011100 (Not approved)
7	Interactive	AF21	010010
8	Interactive	AF11	001010
9	Background	BE	000000

3.6. Protocol Operation

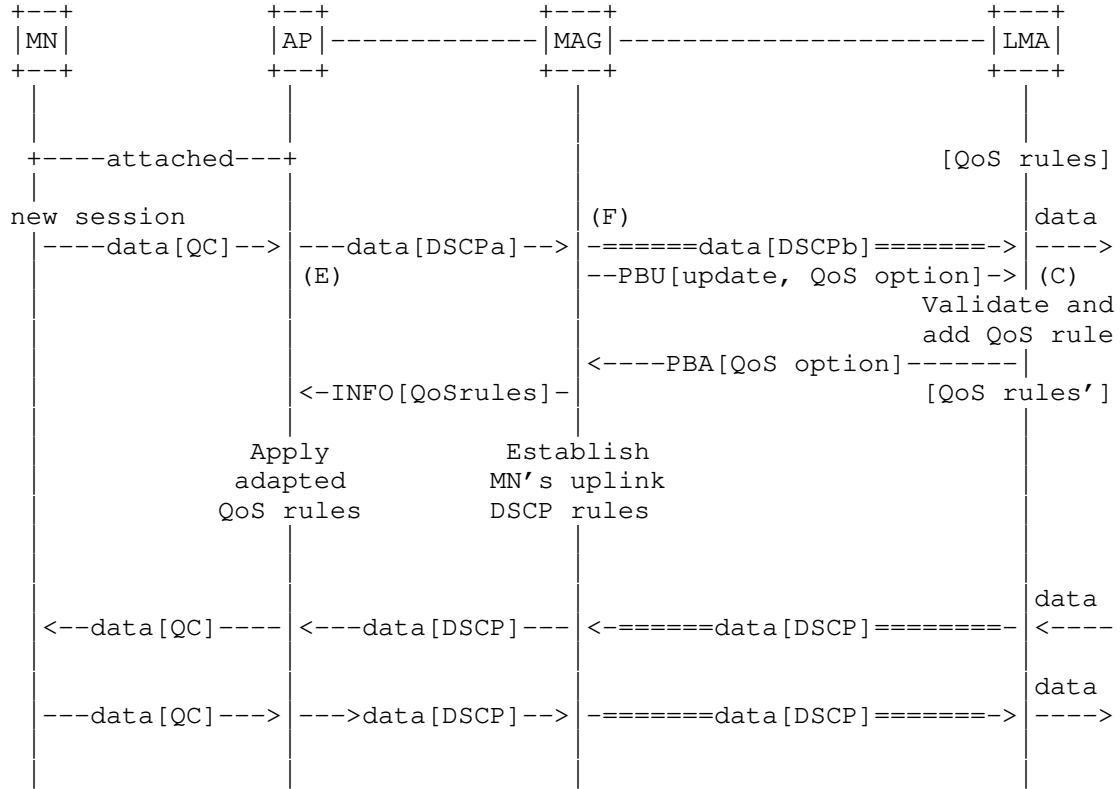
3.6.1. Handover of existing QoS rules



- (A): Apply DSCP at link to AP
 (B): Enforce mapped QoS rules to access technology
 (C): Map MN-indicated QoS Class (QC) to DSCP on the AP-MAG link, or validate MN-indicated QC and apply DSCP on the AP-MAG link according to rule
 (D): Validate received DSCP and apply DSCP according to rule

Figure 4: Handover of QoS rules

3.6.2. Establishment of QoS rules



- (E): AP may enforce uplink QoS rules according to priority class set by the MN
- (F): MAG can enforce a default QoS class until LMA has classified the new flow (notified with PBA) or MAG classifies new flow and proposes the associated QoS class to the LMA for validation (proposed with PBU, notification of validation result with PBA)

Figure 5: Adding new QoS profile for MN initiated flow

4. Protocol Considerations

For supporting this specification, there are protocol extensions needed on both the local mobility anchor and mobile access gateway. The following sections identify those extensions.

4.1. Mobile Access Gateway Considerations

The conceptual Binding Update List entry data structure maintained by the mobile access gateway, described in Section 6.1 of [RFC5213], MUST be extended to store the QoS parameters received from the local mobility anchor. QoS parameters can apply either to the flow or to the mobility session or to the mobile node. Specifically, the following parameters must be defined.

1. Flow Selectors (if QoS parameters are expected to apply at the flow level)
2. DSCP Value
3. List of QoS parameters encoded in TLV format

If a mobile access gateway is enabled to support Quality of Service option, upon accepting a Proxy Binding Acknowledgement with Quality of Service option, it SHOULD update the Binding Update List for that mobility session with the quality of service parameters received from the local mobility anchor. However, if the mobile access gateway is not enabled to support Quality of Service option, it SHOULD just skip the option and continue to process the rest of the message.

The mobility access gateway SHOULD enforce the Quality of Service rules on the mobile node's uplink and downlink traffic as notified by the local mobility anchor. The traffic selectors in the received Quality of Service option are to be used for the flow identification. The DSCP field in the option along with the other parameters in the QoS Information field are to be used for the flow treatment.

In deployments where the mobile access gateway is collocated with a WLAN controller, there is interworking needed between the two functions for exchanging the Quality of Service parameters. The WLAN controller can potentially deliver the Quality of Service parameters to the Access Point/WTP over CAPWAP or other control protocol interface. The specific details on how that is achieved is outside the scope of this document.

4.2. Local Mobility Anchor Considerations

The conceptual Binding Cache entry data structure maintained by the local mobility anchor, described in Section 5.1 of [RFC5213], MUST be extended to store the Quality of Service parameters received from the local mobility anchor. Specifically, the following parameters must be defined.

1. Flow Selectors
2. DSCP Value
3. List of parameters encoded in TLV format

Upon accepting a Proxy Binding Update message [RFC5213] from a mobile access gateway, and if the local mobility anchor is enabled to enforce the Quality of Service rules, it SHOULD construct the Quality of Service mobility option and include it in the Proxy Binding Acknowledgement message.

The Quality of Service MUST be constructed as specified in Section 5. The flow selectors and the parameters for flow treatment MUST be included in the option only if QoS policy is expected to apply at the flow level.

The local mobility anchor SHOULD enforce the Quality of Service rules on the mobile node's uplink and downlink traffic as specified for that mobility session.

5. Quality of Service Option

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

The alignment requirement for this option is 4n.

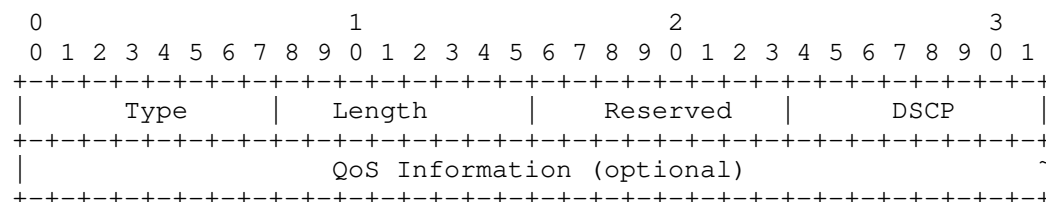


Figure 6: QoS Option

- o Type: To be assigned by IANA
- o Length: 8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields.
- o Reserved : This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.
- o DSCP: An 6-bit unsigned integer indicating the code point value, as defined in [RFC2475] to be used for the flow.
- o QoS Information: one or more Type-Length-Value (TLV) encoded QoS policies. The interpretation and usage of the QoS information is specific to the TLV.

6. Format of the Quality of Service Attribute

The QoS Attribute are used for carrying QoS policy attributes. These sub-options can be included in the QoS option defined in Section 5. The format of this sub-option is as follows.

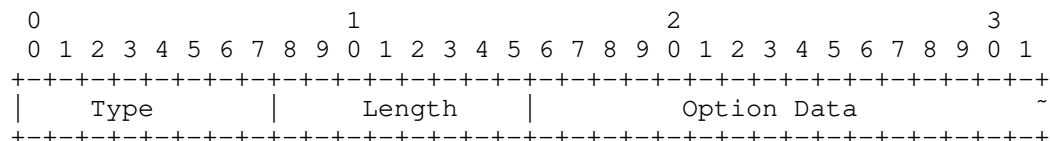


Figure 7: Quality of Service Attribute

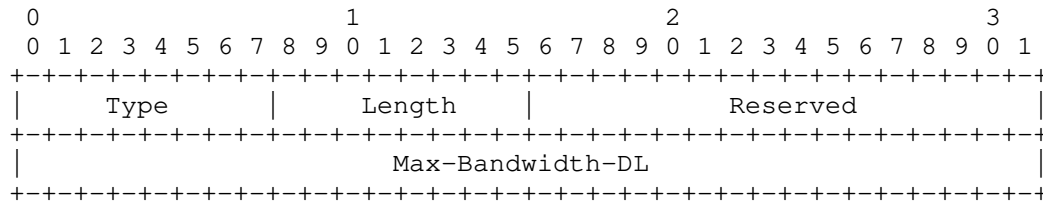
QoS Attribute Type: 8-bit unsigned integer indicating the type of the QoS Attribute.

- 0 - Reserved
- 1 - Per Mobile Node Aggregate Maximum Downlink Bit Rate
- 2 - Per Mobile Node Aggregate Maximum Uplink Bit Rate
- 3 - Per Mobility Session Aggregate Maximum Downlink Bit Rate
- 4 - Per Mobility Session Aggregate Maximum Uplink Bit Rate
- 5 - Allocation and Retention Priority
- 6 - Guaranteed Downlink Bit Rate
- 7 - Guaranteed Uplink Bit Rate
- 8 - Traffic Selector

Length: 8-bit unsigned integer indicating the number of octets needed to encode the Option Data, excluding the Type and Length fields.

6.1. Per Mobile Node Aggregate Maximum Downlink Bit Rate

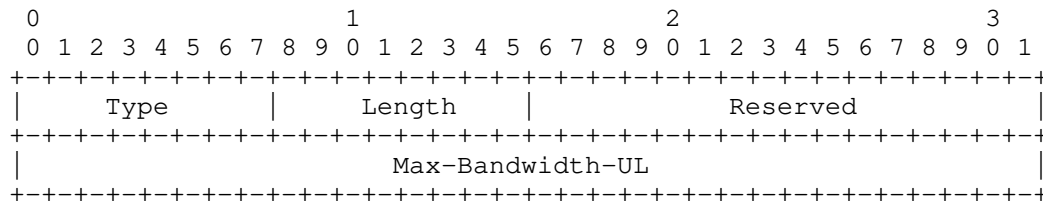
The maximum downlink bit rate for a single Mobile Node. The maximum is an aggregate of all mobility session the Mobile Node has. When provided in a request, it indicates the maximum requested bandwidth. When provided in an answer, it indicates the maximum bandwidth accepted.



- o Type: 1
- o Length: The length of following data value in octets. Set to 6.
- o Max-Bandwidth-DL: is of type unsigned 32 bit integer, and it indicates the maximum bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

6.2. Per Mobile Node Aggregate Maximum Uplink Bit Rate

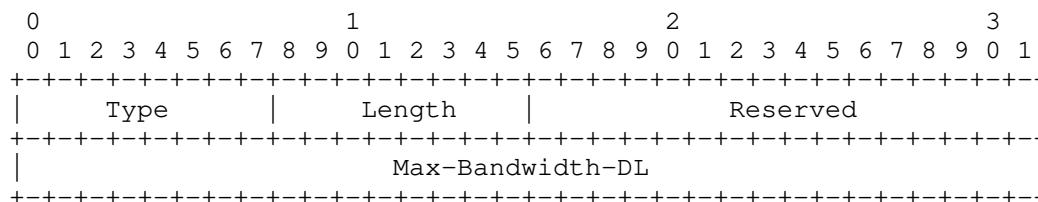
The maximum uplink bit rate for a single Mobile Node. The maximum is an aggregate of all mobility session the Mobile Node has. When provided in a request, it indicates the maximum requested bandwidth. When provided in an answer, it indicates the maximum bandwidth accepted.



- o Type: 2
- o Length: The length of following data value in octets. Set to 6.
- o Max-Bandwidth-UL: is of type unsigned 32 bit integer, and it indicates the maximum bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

6.3. Per Mobility Session Aggregate Maximum Downlink Bit Rate

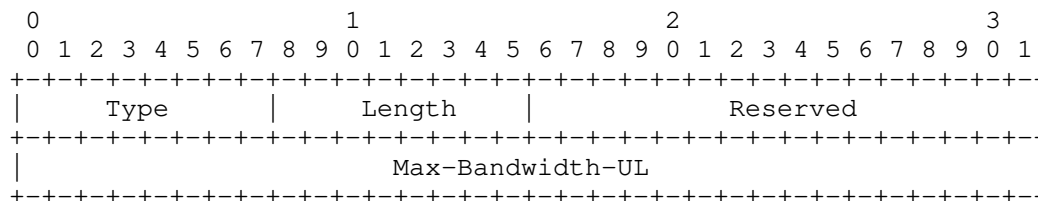
The maximum downlink bit rate for a single specific mobility session the Mobile Node has. When provided in a request, it indicates the maximum requested bandwidth. When provided in an answer, it indicates the maximum bandwidth accepted.



- o Type: 3
- o Length: The length of following data value in octets. Set to 6.
- o Max-Requested-Bandwidth-DL: is of type unsigned 32 bit integer, and it indicates the maximum bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

6.4. Per Mobility Session Aggregate Maximum Uplink Bit Rate

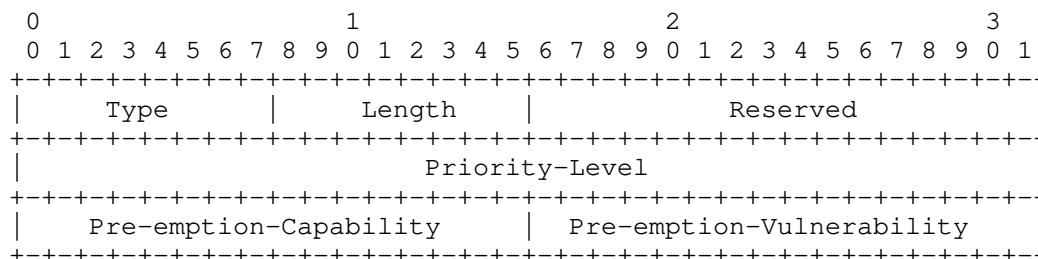
The maximum uplink bit rate for a single specific mobility session the Mobile Node has. When provided in a request, it indicates the maximum requested bandwidth. When provided in an answer, it indicates the maximum bandwidth accepted.



- o Type: 4
- o Length: The length of following data value in octets. Set to 6.
- o Max-Bandwidth-UL: is of type unsigned 32 bit integer, and it indicates the maximum bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

6.5. Allocation and Retention Priority

The allocation and retention priority indicate the priority of allocation and retention for the corresponding mobility session or flow. The traffic selector (Section 6.8) MUST be included in the QoS option when the QoS rule is expected to be applied at flow level.



- o Type: 5
- o Length: The length of following data values in octets. Set to 10.
- o Priority-Level: is of type unsigned 32 bit integer, and it used for deciding whether a mobility session establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The priority-level can also be used to decide which existing mobility session to pre-empt during resource limitations. The priority level defines the relative importance of a resource request.

Values 1 to 15 are defined, with value 1 as the highest level of priority.

Values 1 to 8 should only be assigned for services that are authorized to receive prioritized treatment within an operator domain. Values 9 to 15 may be assigned to resources that are authorized by the home network and thus applicable when a MN is roaming.

- o Pre-emption-Capability: defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level. The following values are defined:

Enabled (0): This value indicates that the service data flow is allowed to get resources that were already assigned to another IP data flow with a lower priority level.

Disabled (1): This value indicates that the service data flow is not allowed to get resources that were already assigned to another IP data flow with a lower priority level.

- o Pre-emption-Vulnerability: defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level. The following values are

defined:

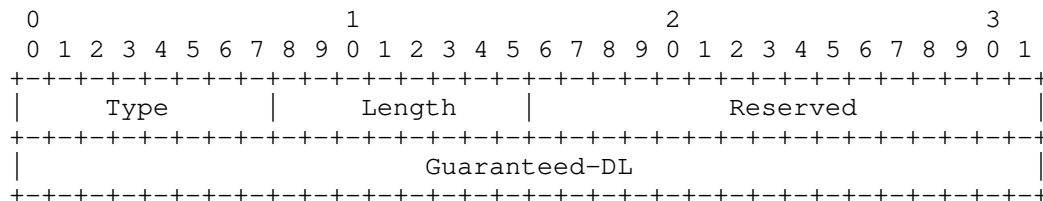
Enabled (0): This value indicates that the resources assigned to the IP data flow can be pre-empted and allocated to a service data flow with a higher priority level.

Disabled (1): This value indicates that the resources assigned to the IP data flow shall not be pre-empted and allocated to a service data flow with a higher priority level.

6.6. Guaranteed Downlink Bit Rate

The guaranteed downlink bit rate for a specific flow or mobility session the Mobile Node has. When provided in a request, it indicates the maximum requested bandwidth. When provided in an answer, it indicates the maximum bandwidth accepted.

The traffic selector (Section 6.8) MUST be included in the QoS option when the QoS rule is expected to be applied at flow level.

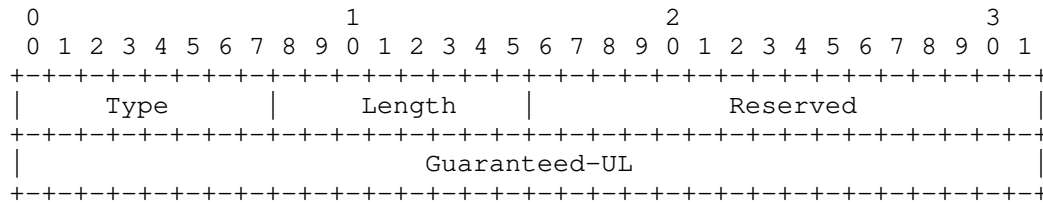


- o Type: 6
- o Length: The length of following data value in octets. Set to 6.
- o Guaranteed-DL: is of type unsigned 32 bit integer, and it indicates the guaranteed bandwidth in bits per second for downlink IP flows. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

6.7. Guaranteed Uplink Bit Rate

The guaranteed downlink bit rate for a specific flow or mobility session the Mobile Node has. When provided in a request, it indicates the maximum requested bandwidth. When provided in an answer, it indicates the maximum bandwidth accepted.

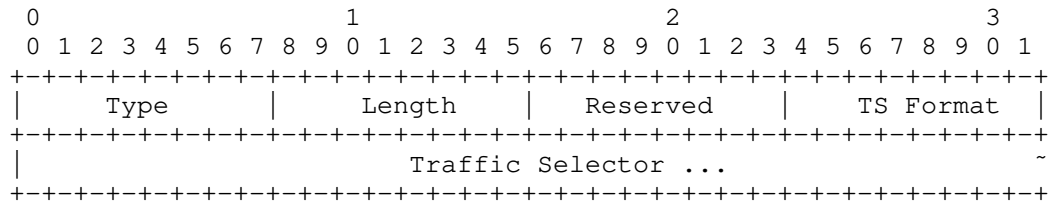
The traffic selector (Section 6.8) MUST be included in the QoS option when the QoS rule is expected to be applied at flow level.



- o Type: 7
- o Length: The length of following data value in octets. Set to 6.
- o Guaranteed-UL: is of type unsigned 32 bit integer, and it indicates the guaranteed bandwidth in bits per second for uplink IP flows. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

6.8. Traffic Selector

MUST be included if QoS parameters (Options according to Section 6.5 to Section 6.7) are expected to apply at the flow level



- o Type: 8
- o Length: The length of following data value in octets.
- o TS Format: An 8-bit unsigned integer indicating the Traffic Selector Format. Value "0" is reserved and MUST NOT be used. The value of (1) is assigned for IPv4 Binary Traffic Selector, as defined in section 3.1 of [RFC6088].
- o Traffic Selector: variable-length opaque field for including the traffic specification identified by the TS format field.

7. IANA Considerations

This document requires the following IANA actions.

- o Action-1: This specification defines a new Mobility Header option, the Quality of Service (QoS) option. The format of this option is described in Section 5. The Type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options, as defined in [RFC6275].
- o Action-2: This specification defines a new mobility sub-option format, Quality of Service Attribute. The format of this mobility sub-option is described in Section 6. This sub-option can be carried in Quality of Service option. The type values for this sub-option needs to be managed by IANA, under the Registry, Quality of Service Attribute Registry. This specification reserves the following type values. Approval of new Quality of Service Attribute type values are to be made through IANA Expert Review.

0 - Reserved

1 - Per Mobile Node Aggregate Maximum Downlink Bit Rate

2 - Per Mobile Node Aggregate Maximum Uplink Bit Rate

3 - Per Mobility Session Aggregate Maximum Downlink Bit Rate

4 - Per Mobility Session Aggregate Maximum Uplink Bit Rate

5 - Allocation and Retention Priority

6 - Guaranteed Downlink Bit Rate

7 - Guaranteed Uplink Bit Rate

8 - Traffic Selector

8. Security Considerations

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

9. Acknowledgements

The authors of this document thank the NetExt Working Group for the valuable feedback to different versions of this specification. In particular the authors want to thank Basavaraj Patil, Behcet Sarikaya, Charles Perkins, Dirk von Hugo, Mark Grayson, Tricci So and Ahmad Muhanna for their valuable comments and suggestions to improve this specification.

10. References

10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [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.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.
- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

10.2. Informative References

- [80211e] IEEE, "IEEE part 11: Wireless LAN Medium Access Control(MAC) and Physical Layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements", 2005.
- [GSMA.IR.34] GSMA, "Inter-Service Provider IP Backbone Guidelines 5.0", February 2012.
- [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-05 (work in progress), June 2013.
- [RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.
- [RFC5845] Muhanna, A., Khalil, M., Gundavelli, S., and K. Leung, "Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6", RFC 5845, June 2010.
- [RFC5846] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K., and P. Yegani, "Binding Revocation for IPv6 Mobility", RFC 5846, June 2010.

[TS23.402]

3GPP, "Architecture enhancements for non-3GPP accesses",
2010.

Appendix A. Information when implementing PMIP based QoS support with IEEE 802.11e

This section shows, as an example, the end-to-end QoS management with a 802.11e capable WLAN access link and a PMIP based QoS support.

The 802.11e, or Wi-Fi Multimedia (WMM), specification provides prioritization of packets for four types of traffic, or access categories (AC):

Voice (AC_VO): Very high priority queue with minimum delay. Time-sensitive data such as VoIP and streaming mode are automatically sent to this queue.

Video (AC_VI): High priority queue with low delay. Time-sensitive video data is automatically sent to this queue.

Best effort (AC_BE): Medium priority queue with medium throughput and delay. Most traditional IP data is sent to this queue.

Background (AC_BK): Lowest priority queue with high throughput. Bulk data that requires maximum throughput but is not time-sensitive (for example, FTP data) is sent to the queue.

The access point uses the 802.11e indicator to prioritize traffic on the WLAN interface. On the wired side, the access point uses the 802.1p priority tag and DiffServ code point (DSCP). To allow consistent QoS management on both wireless and wired interfaces, the access point relies on the 802.11e specification which define mapping between the 802.11e access categories and the IEEE 802.1D priority (802.1p tag). The end-to-end QoS architecture is depicted on Figure 8 and the 802.11e/802.1D priority mapping is reminded in the following table:

802.1e AC	802.1D priority
AC_VO	7, 6
AC_VI	5, 4
AC_BE	0, 3
AC_BK	2, 1

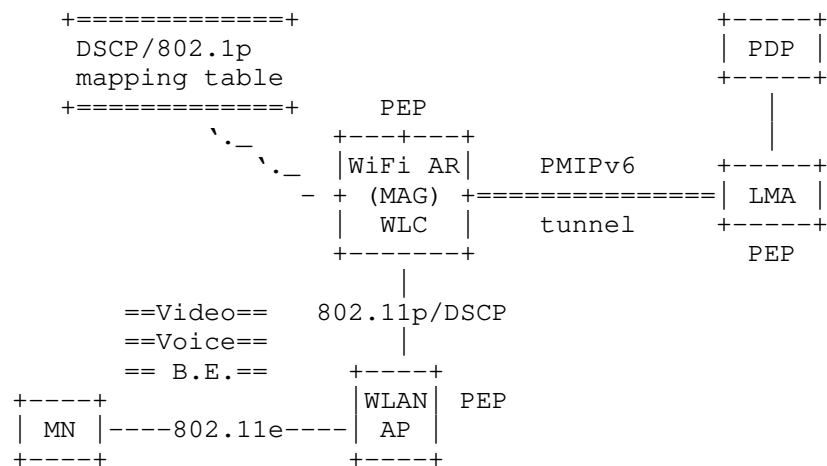


Figure 8: End-to-end QoS management with 802.11e

When receiving a packet from the MN, the AP checks whether the frame contains 802.11e markings in the L2 header. If not, the AP checks the DSCP field. If the uplink packet contains the 802.11e marking, the access point maps the access categories to the corresponding 802.1D priority as per the table above. If the frame does not contain 802.11e marking, the access point examines the DSCP field. If DSCP is present, the AP maps DSCP values to a 802.1p value (i.e 802.1D priority). This mapping is not standardized and may differ between operator; a mapping example given in the following table.

Type of traffic	802.1p	DSCP value
Network Control	7	56
Voice	6	46 (EF)
Video	5	34 (AF 41)
voice control	4	26 (AF 31)
Background Gold	2	18 (AF 21)
Background Silver	1	10 (AF 11)
Best effort	0,3	0 (BE)

The access point prioritizes ingress traffic on the Ethernet port

based on the 802.1p tag or the DSCP value. If 802.1p priority tag is not present, the access point checks the DSCP/802.1p mapping table. The next step is to map the 802.1p priority to the appropriate egress queue. When 802.11e support is enabled on the wireless link, the access point uses the IEEE standardized 802.1p/802.11e correspondence table to map the traffic to the appropriate hardware queues.

When the 802.11e capable client sends traffic to the AP, it usually marks packets with a DSCP value. In that case, the MAG/LMA can come into play for QoS renegotiation and call flows depicted in Section 3.6 apply. Sometimes, when communication is initiated on the WLAN access, the application does not mark upstream packets. If the uplink packet does not contain any QoS marking, the AP/MAG could determine the DSCP field according to traffic selectors received from the LMA. Figure 9 gives the call flow corresponding to that use-case and shows where QoS tags mapping does come into play. The main steps are as follows:

(A): during MN attachment process, the MAG fetches QoS policies from the LMA. After this step, both MAG and LMA are provisioned with QoS policies.

(B): the MN starts a new IP communication without making IP packets with DSCP tags. The MAG uses the traffic selector to determine the DSCP value, then it marks the IP packet and forwards within the PMIP tunnel.

(C): the LMA checks the DSCP value with respect to the traffic selector. If the QoS policies is valid, the LMA forwards the packet without renegotiate QoS rules.

(D): when receiving a marked packet, the MAG, the AP and the MN use 802.11e (or WMM), 802.1p tags and DSCP values to prioritize the traffic.

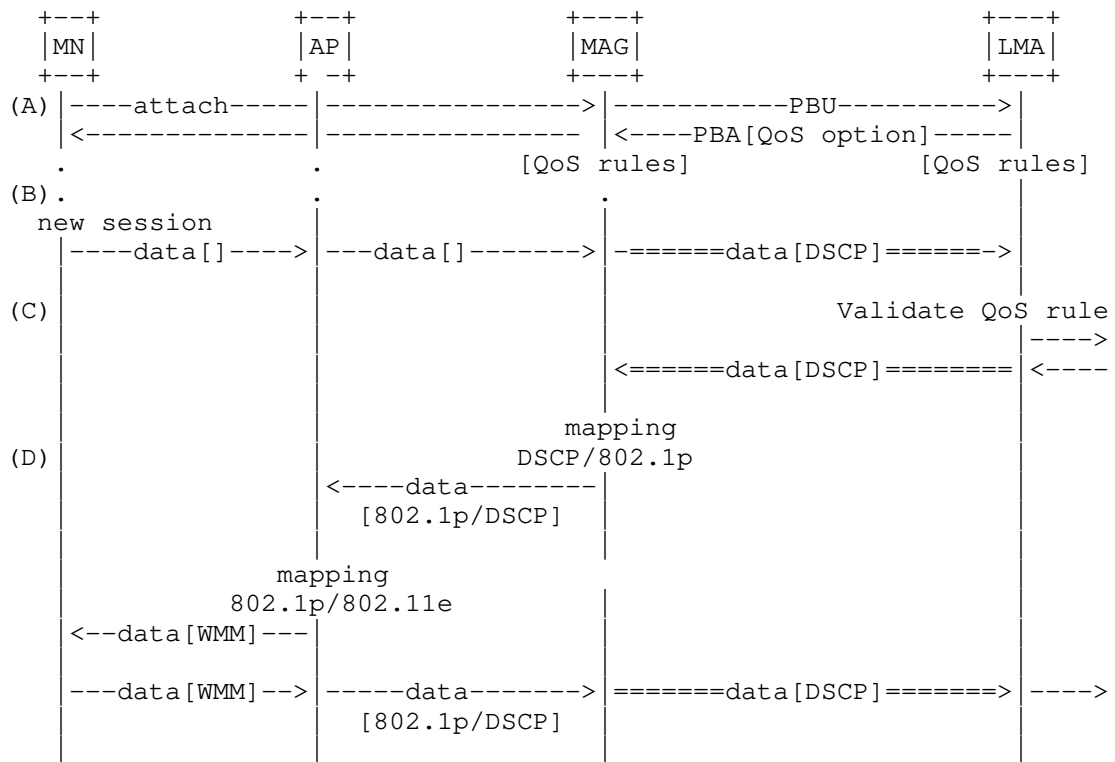


Figure 9: Prioritization of a flow created on the WLAN access

Authors' Addresses

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

Email: liebsch@neclab.eu

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

Email: pierrick.seite@orange.com

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

Email: yokota@kddilabs.jp

Jouni Korhonen
Renesas Mobile
Porkkalankatu 24
Helsinki FIN-00180
Finland

Email: jouni.nospam@gmail.com

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

Email: sgundave@cisco.com

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

CJ. Bernardos, Ed.
UC3M
March 18, 2016

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

Abstract

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

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

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

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

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

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

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

Copyright Notice

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

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

Table of Contents

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

1. Introduction

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

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

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

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

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

Local Mobility Agent (LMA).

Mobile Access Gateway (MAG).

Proxy Mobile IPv6 Domain (PMIPv6-Domain).

LMA Address (LMAA).

Proxy Care-of Address (Proxy-CoA).

Home Network Prefix (HNP).

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

Binding Identification Number (BID).

Flow Identifier (FID).

Traffic Selector (TS).

The following terms are defined and used in this document:

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

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

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

3. Overview of the PMIPv6 flow mobility extensions

3.1. Use case scenarios

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

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

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

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

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

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

3.2. Basic Operation

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

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

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

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

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

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

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

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

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

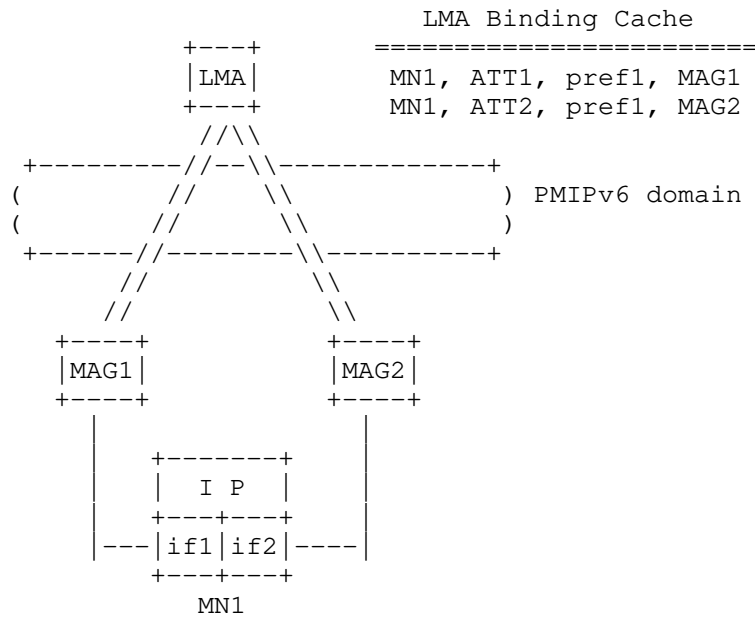


Figure 1: Shared prefix across physical interfaces scenario

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

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

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

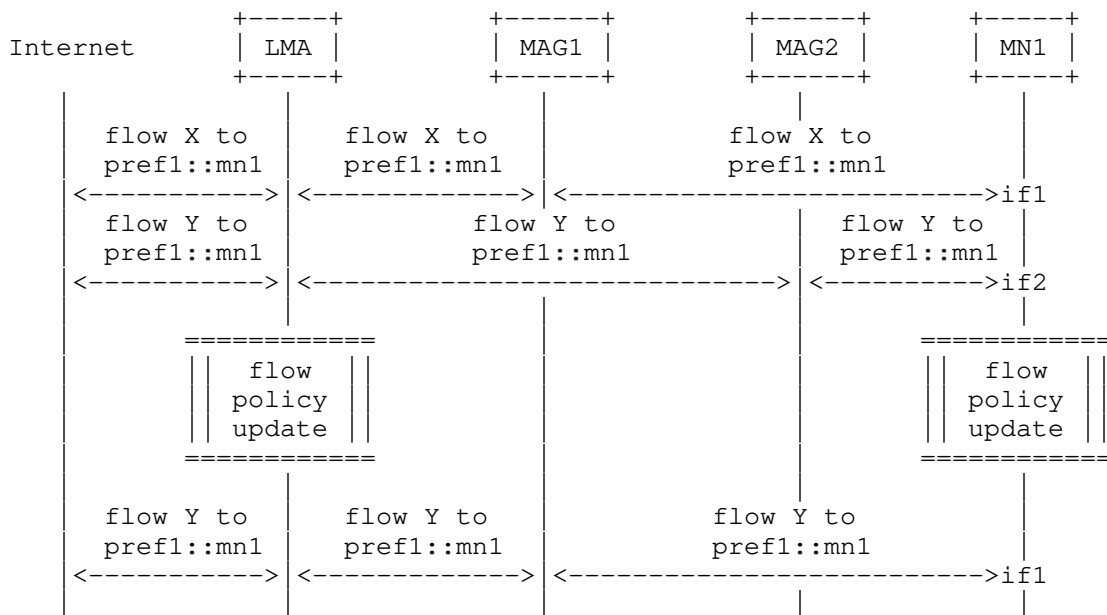


Figure 2: Flow mobility message sequence with common set of prefixes

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

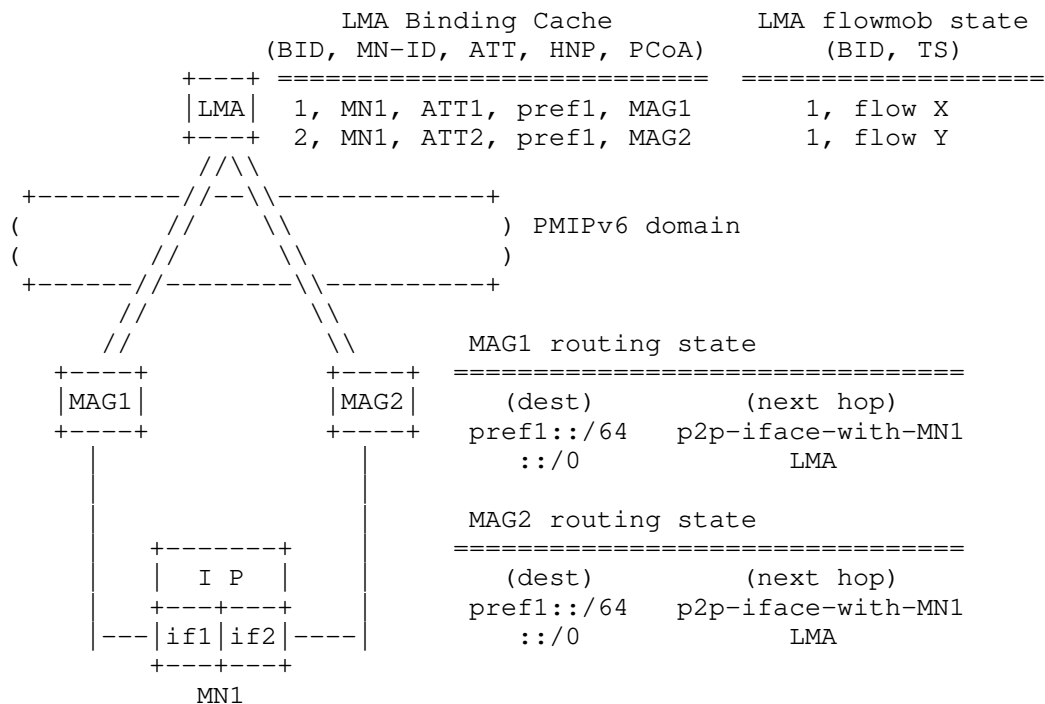


Figure 3: Data structures with common set of prefixes

3.2.2. MN with different sets of prefixes on each MAG

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

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

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

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

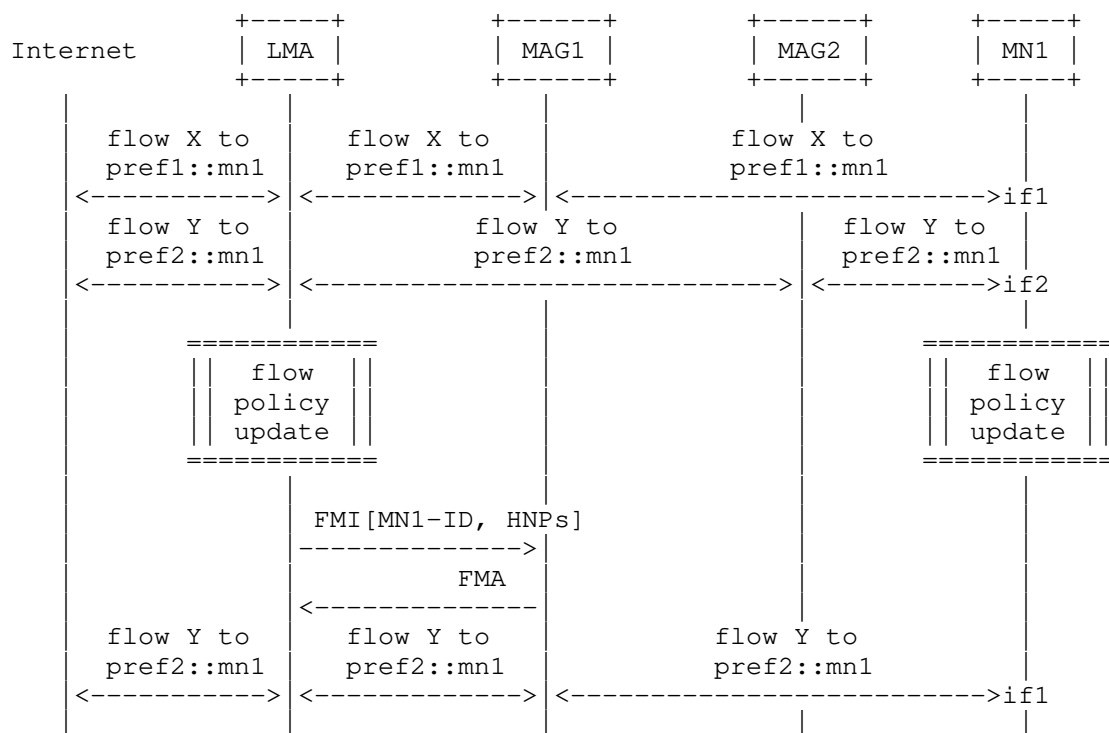


Figure 4: Flow mobility message sequence when the LMA assigns different sets of prefixes per physical interface

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

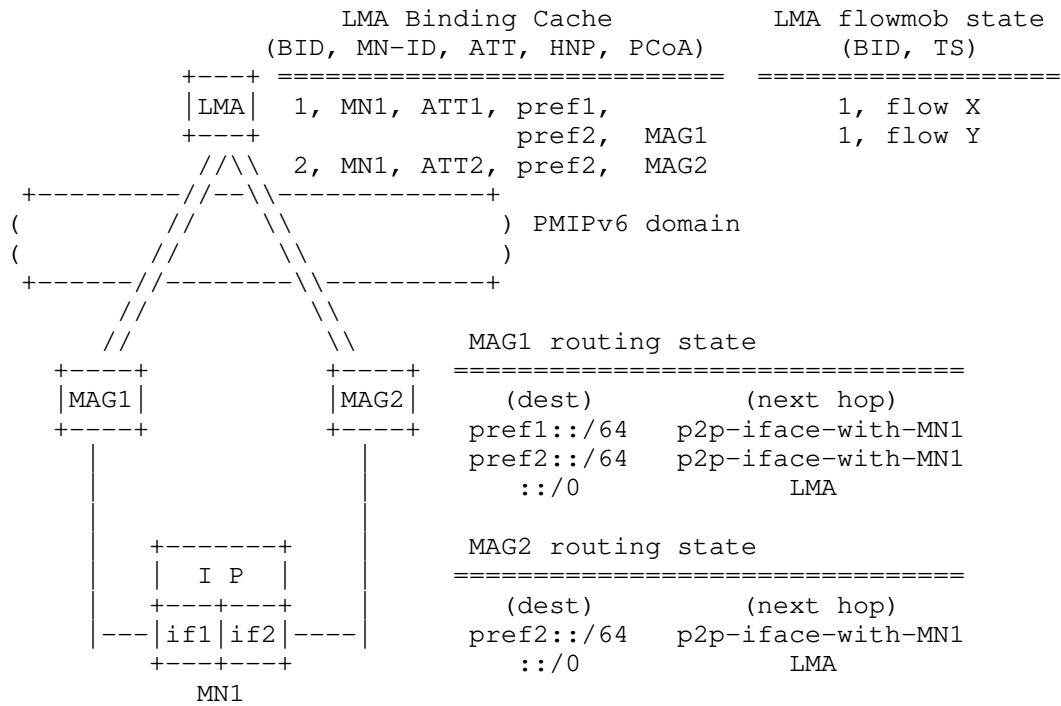


Figure 5: Data structures when the LMA assigns a different set of prefixes

3.3. Use of PBU/PBA signaling

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

3.4. Use of flow-level information

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

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

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

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

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

4. Message Formats

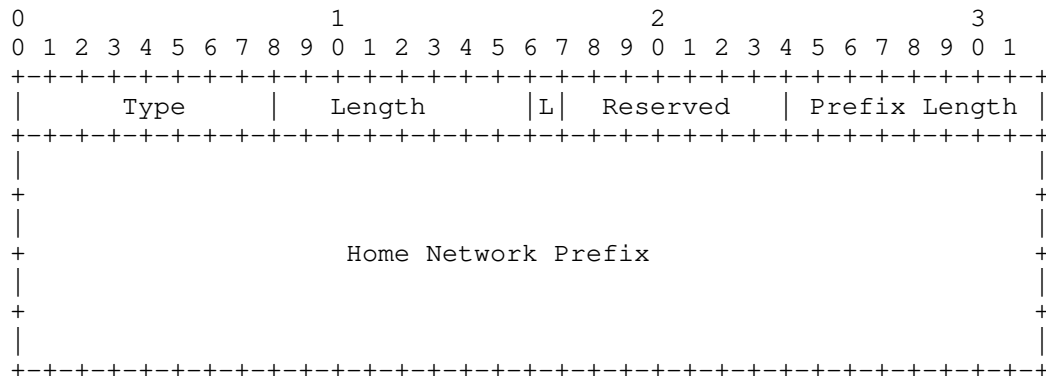
This section defines modifications to the Proxy Mobile IPv6 [RFC5213] protocol messages.

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

4.1. Home Network Prefix

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

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



Off-link Home Network Prefix Flag (L):

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

4.2. Flow Mobility Initiate (FMI)

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

Notification Reason:

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

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

4.3. Flow Mobility Acknowledgement (FMA)

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

Status Code:

0: Success.

{IANA-2}: Reason unspecified.

{IANA-3}: MN not attached.

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

5. Conceptual Data Structures

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

5.1. Multiple Proxy Care-of Address Registration

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

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

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

Figure 6: Extended Binding Cache

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

5.2. Flow Mobility Cache

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

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

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

Figure 7: Flow Mobility Cache

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

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

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

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

6. Mobile Node considerations

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

7. IANA Considerations

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

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

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

8. Security Considerations

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

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

9. Authors

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

Kuntal Chowdhury

E-mail: kc@alttiostar.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

Rajeev Koodli

E-mail: rajeevkoodli@google.com

Telemaco Melia

E-mail: telemaco.melia@googlemail.com

Frank Xia

E-mail: xiayangsong@huawei.com

10. Acknowledgments

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

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

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

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

11. References

11.1. Normative References

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

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

11.2. Informative References

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

Author's Address

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

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: <http://www.it.uc3m.es/cjbc/>

INTERNET-DRAFT
Intended Status: Informational
Expires: October 23, 2013

John Kaippallimalil
Huawei
April 21, 2013

Mapping PMIP Quality of Service in WiFi Network
draft-kaippallimalil-netext-pmip-qos-wifi-02

Abstract

This document proposes a model for configuring and mapping PMIP QoS parameters of a mobile network session to the corresponding connection at a WiFi Access Point. In congested network conditions, it is useful for an MN's flows to be policed and shaped at the WLC and WiFi AP to match bandwidth constraints or service priority of the user's subscription. Applying similar QoS management at the WiFi AP and WLC allows optimal use of network resources. Currently, the WiFi AP does not have information on the MNs subscribed bandwidth, or relative priority of its flows or services for per user QoS handling at the WiFi AP. This document provides a model for mapping PMIP QoS to corresponding 802.11e QoS parameters.

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	4
1.2. Definitions	4
1.3. Abbreviations	4
2. QoS Mechanisms	4
2.1. QoS in Mobile Networks	4
2.2. QoS in WiFi Networks	5
3. Connection Model	5
4. Policy Provisioning Architecture	7
5. QoS Configuration and Mapping	8
5.1. PMIP - 802.11e QoS Configuration	8
5.2. Mapping Recommendations and Default Values	9
6. Next Steps	10
7. Security Considerations	11
8. IANA Considerations	11
9. References	11
9.1. Normative References	11
9.2. Informative References	11
Authors' Addresses	12

1. Introduction

This document describes a means for the QoS profile of a PMIP session to be applied to QoS on the 802.11 connection segment of the MN (Mobile Node). A mobile network may dynamically provision QoS for its users attached via a WiFi access and PMIP backhaul. [PMIP-QoS] defines a mechanism by which QoS policy parameters in the mobile network are delivered from the LMA to the the WLC (MAG) using PMIP QoS extensions. [PMIP-QoS] further describes how the DSCP value for the PMIP session is mapped to corresponding 802.1p value that may be used by IP backhaul network or WiFi APs to prioritize IP flows of a host (MN).

While [PMIP-QoS] defines how mobile network QoS can be applied to PMIP flows, the WiFi AP has to reflexively map QoS for IP flows. Based on the observed DSCP values in downstream packets of an IP flow, the WiFi AP provides the same level of QoS in the upstream direction. In addition, the WiFi AP may use the downstream DSCP values to determine the scheduling priority in the 802.11 network. Based on [PMIP-QoS], the WLC (MAG) can use DSCP priority as well as other parameters of the MN such as subscribed bandwidth and service priority to police IP flows of an MN. The WiFi AP on the other hand relies on DSCP priority for scheduling and policing IP flows of an MN since it does not have per subscriber policy information of an MN. In congested network conditions, it is not possible for the WiFi AP to differentiate between MNs that have premium subscriptions. In addition, it is possible that upstream flows from the WiFi AP are throttled by the WLC to match the bandwidth constraints or service priority. This can result in sub-optimal use of network resources. In order for the WiFi AP to differentiate on per flow and per user basis, it needs information on the MNs subscribed bandwidth and other policy information.

This proposal aims to provide the WiFi AP with per MN QoS profile to allow more effective overall use of network resources - both WiFi radio and IP backhaul. The QoS parameters needed are available to the WLC during MN authorization and establishment of the PMIP session with QoS extensions. Since an MN may establish tunneled IP flows, direct IP connections or offloaded connections, the relationship of PMIP QoS to 802.11e QoS is explained. It is possible that an MN (with a single 802.11 interface) has more than one PMIP session. The QoS policy for the MN may be applied by the AP to schedule and control WiFi radio network resources and upstream user flows in the IP backhaul network. If per session QoS policy is not available, the AP may be provisioned to apply QoS based on the subscribed QoS values obtained during 3GPP user authorization.

In order to provision QoS in the WiFi network, a consistent mapping

of QoS parameters and values between 3GPP and 802.11e is needed. Recommendations to map 3GPP QCI to DSCP for mobility sessions are available in [PMIP-QoS]. This document adds the configuration of QoS per PMIP mobility session to a WiFi radio access.

The rest of the document is organized as follows. Chapter 2 outlines the QoS mechanisms in 3GPP mobile networks and 802.11 networks. Chapter 3 provides an overview of the architecture in which QoS is provisioned on the WiFi AP. Chapters 4 and 5 describe the connection model in the access network and the QoS mapping itself.

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

1.3. Abbreviations

3GPP	Third Generation Partnership Project
AAA	Authentication Authorization Accounting
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. QoS Mechanisms

2.1. QoS in Mobile 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 [TS23.401]. 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].

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 WiFi Networks

802.11e [802.11e] defined by IEEE provides an enhancement of the MAC layer in WiFi networks to support QoS. Basic 802.11 WiFi uses CSMA and collision avoidance to provide best effort access to the medium. 802.11e defines a Hybrid Coordination Function (HCF) that provides a priority based access and also admission control based access.

HCF contention based channel access provides prioritized access to the 802.11 medium. Four access categories (AC) are defined based on traffic type. Each arriving frame is mapped into one of four FIFO queues corresponding to different user priority (UP) values. The highest priority frame is transmitted when access is obtained in a contention window. Access categories and their mapping to 802.1D user priorities is provided [802.11e].

HCF controlled channel access uses a central coordinator to provide contention free access to the medium based on admission control. The HCCA (HCF Controlled Channel Access) based scheduling can use configured policies to grant exclusive access to a QSTA (user) for limited contention free slots.

3. Connection Model

MNs that attach to a mobile network via a WiFi AP and WLC are provisioned with IP addresses corresponding to each PMIP session. Each of the IP sessions at MN has QoS policies associated to it. This section outlines the connection model in detail and QoS mapping on the WiFi AP.

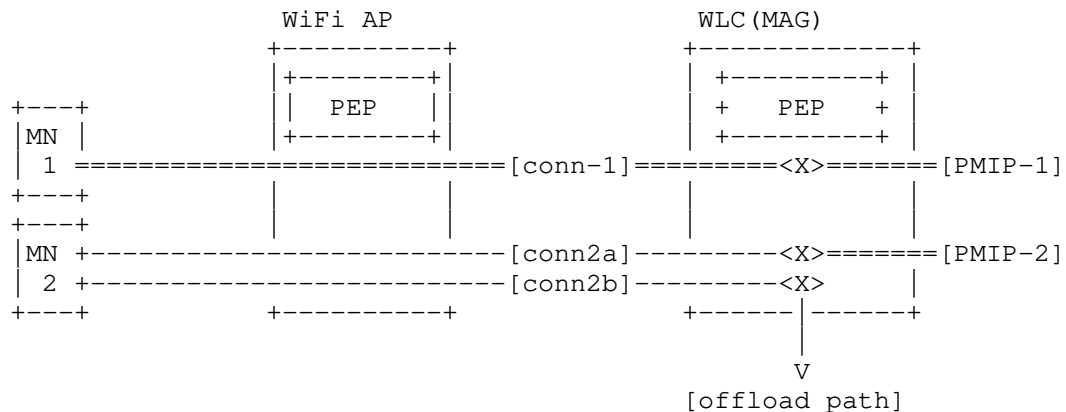


Figure 1: MN Connection model

An MN may establish a session to the mobile network or may have a session that is offloaded to the internet from the WLC. Figure 2 shows MN1 and MN2 attached to the WLC via a WiFi AP. An MN may have a tunneled connection to the mobile network (MN1, conn-1, PMIP-1), (MN2, conn2a, PMIP-2) and an IP connection that is offloaded at the WLC (MN2, conn2b, offload). The specification for IP tunnel/connection between MN and WLC are out of the scope of this document.

For an MN - WLC connection segment with IP address configured via PMIP (e.g. MN2 conn2a), the corresponding PMIP QoS would be applicable to MN flows with this IP address.

For connection segment that is offloaded at WLC, the IP address is configured by the WLC. As in the case of PMIP connections, QoS is provisioned for MN flows with this IP address

In both cases - PMIP session related connection segment, or offload connection segment - the WiFi AP gets QoS traffic filters and configuration from the WLC. The QoS profile would be identified by the IP address for the PMIP / offload session.

4. Policy Provisioning Architecture

This section describes the architecture in which the PMIP QoS configuration of MN sessions is applied to the corresponding traffic flows in the WiFi Access Point. Following MN attach to the WiFi network and authentication with the mobile network, the WLC gets QoS parameters and other policy for the authorized MN. When the PMIP connection is created, the PDN-GW returns QoS policy using [PMIP-QoS] extensions.

In [PMIP-QoS], the Access Point (AP) is not directly provisioned with QoS for an MN connection. As a result, the AP is only able to prioritize flows based on observed downlink DSCP values. Additionally, the AP does not know the maximum bandwidth of a subscriber or flow to be applied on the WiFi radio network. This can result in sub-optimal utilization of scarce WiFi network resources, and of the overall access network. This solution provides a description to provision the AP with QoS policy associated to an MN.

The paragraphs that follow outline the overall architecture and subsequent chapters provide details on QoS parameters provisioned in the AP.

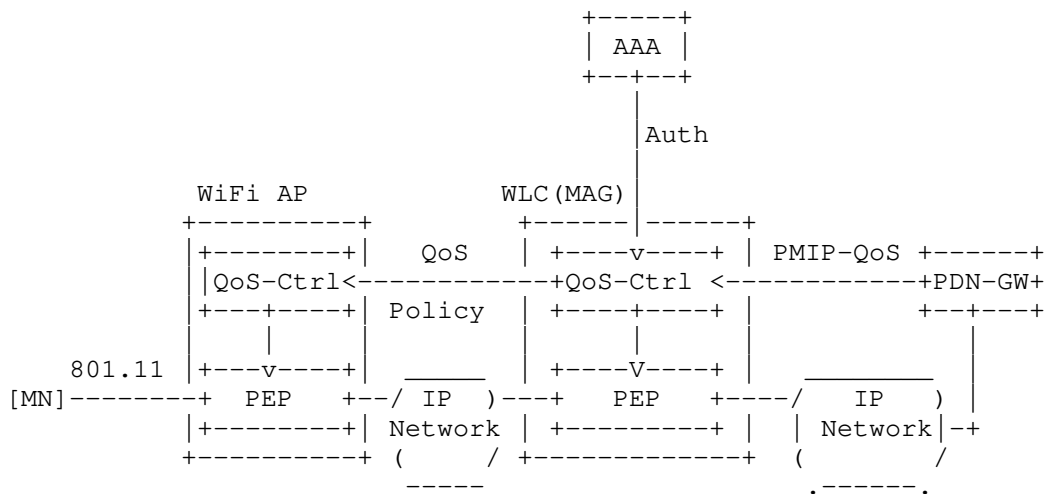


Figure 2: Architecture for provisioning QoS Policy on WiFi AP

Figure 1 provides an overview of the architecture in which QoS for an MN is provisioned on the AP. MN QoS policy from initial session authorization and PMIP connection establishment is provisioned in the WLC QoS-Ctrl (logical function). QoS-Ctrl in WLC installs QoS to the

WLC PEP as described in [PMIP-QoS].

The WLC translates 3GPP QoS policy to equivalent parameters for IP flows and applies them for scheduling and policing.

In this solution, the WLC sends policy information for an MNs PMIP sessions to the WiFi AP. The protocols used to exchange QoS parameters between the WLC and AP are not discussed in this document. The AP can use the received QoS policy configuration and applies them to upstream and downstream forwarding of data packets in the WiFi radio network. The AP can also apply these QoS policies for upstream user IP flows to the WLC.

An MN may have more than one PMIP session at any given time. Each of these PMIP sessions can have different policy parameters. The WLC provides the WiFi AP with a policy corresponding to each of these PMIP sessions. Since each PMIP session configures an IP address for the MN, the policy can be sent per IP address of MN that corresponds to the PMIP session. This model is described further in the following chapter.

If the MN connection at WLC is offloaded to the internet, there is no PMIP session setup to the mobile network. In this case, the WLC should use the subscriber policy obtained during authorization. The WiFi AP is provisioned as for other sessions. The WLC provides the WiFi AP with QoS parameters for the MN IP address used for the offload connection.

5. QoS Configuration and Mapping

5.1. PMIP - 802.11e QoS Configuration

The WiFi Access Point (AP) gets QoS configuration per IP session from the WLC. The QoS information per IP session provided to the AP includes:

- Hardware (MAC) address of host for which PMIP session is established.
- IP prefix or address of PMIP mobility session.
- IP port address (used for NATed connections).
- DSCP. Diffserv PHB value of PMIP QoS for the mobility session.
- QCI. The WLC provides the 3GPP QCI value if available, for example, from authorization profile of APN (i.e. subscribed values per established PMIP mobility session).
- ARP (Allocation and Retention Priority). This value is obtained from the PMIP QoS for the mobility session. It determines the priority of a flow (1 has highest priority).
- MBR (Maximum Bit Rate) for mobility session uplink and downlink. This should not exceed the AMBR (Aggregate MBR) of the

subscription.

- GBR (Guaranteed Bit Rate) for mobility session uplink and downlink, if required.

The WiFi AP uses the above QoS configuration to implement classification, admission control and forwarding of MN flows. The WiFi AP maps DSCP (or QCI) to 802.11e AC (Access Categories) for each IP session / hardware (MAC) address of the host (3GPP user). The mapping from DSCP or QCI to 802.11e AC is shown in table in chapter 4 below.

In the WiFi radio network, the AP uses 802.11e AC values for contention (HCF) based forwarding based on priority. The AP schedules downstream flows in the WiFi radio network and for upstream IP backhaul to the WLC. For contention free scheduling, the WiFi AP additionally uses the QoS configuration per user to admit flows based on 802.11e ADDTS (ADD TSPEC) requests from the host (3GPP user). The WiFi AP may drop packet that fall outside the configured MBR and GBR. In case of severe radio congestion, the WiFi AP can use ARP in addition to DSCP drop precedence to determine the flows to be dropped.

5.2. Mapping Recommendations and Default Values

The table below outlines a recommended mapping between 3GPP QCI, and 802.11e Access Category (AC) priorities. QCI packet delay budget and packet error loss rate may be used by the WiFi access point in scheduling contention free access when HCCA scheduling is used.

QCI	DSCP	802.11e AC	Example 3GPP service
1	EF	3 AC_VO	conversational voice
2	EF	3 AC_VO	conversational video
3	EF	3 AC_VO	real-time gaming
4	AF41	2 AC_VI	buffered streaming
5	AF31	2 AC_VI	IMS signaling
6	AF31	2 AC_VI	buffered streaming
7	AF21	0 AC_BE	interactive gaming
8	AF11	0 AC_BE	web access
9	BE	1 AC_BK	e-mail

Table 1: QoS Mapping between QCI, WMM, 802.11e AC

6. Next Steps

This document has described a basic model for mapping PMIP QoS parameters to 802.11e parameters. However, there are a few questions that need to be explored further.

The protocol between WLC and AP is not discussed in this document. There needs to be work to determine the protocol specification if it is desired that WLC and AP should interwork for QoS capability.

Another aspect is this draft does not describe multiple PDN connections per MN in much detail. This is work in progress in 3GPP and the results should be compatible with the model in this draft.

RTC Web impact to 3GPP networks is currently being studied. There are several technical options being considered by 3GPP at this time. If the chosen solution requires more than one type of DSCP/QoS to be configured per PMIP session/IP connection segment - for example if audio and video flows use the same IP session - then this capability is required for WLC - AP configuration also.

Finally, the QoS values listed in the table in chapter 5 needs to be aligned with [PMIP-QoS] and GSMA.

7. Security Considerations

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

8. IANA Considerations

No IANA assignment of parameters are required in this document.

9. References

9.1. 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.

9.2. 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.
- [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).
- [TS23.401] General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 11), 3GPP TS 23.401, V11.2.0 (2012-06).
- [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).
- [802.11e] IEEE, "IEEE part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements" 802.11e-2005, 22 September 2005.
- [GSMA-IR34] Inter-Service Provider Backbone Guidelines 5.0, 22 December 2010

Authors' Addresses

John Kaippallimalil
5340 Legacy Drive, Suite 175
Plano Texas 75024

E-Mail: john.kaippallimalil@huawei.com

NETEXT WG
Internet-Draft
Intended status: Standards Track
Expires: January 17, 2014

R. Wakikawa
Softbank Mobile
R. Pazhyannur
S. Gundavelli
Cisco
July 16, 2013

Separation of Control and User Plane for Proxy Mobile IPv6
draft-wakikawa-netext-pmip-cp-up-separation-00.txt

Abstract

This document describes splitting of Control Plane (CP) and User Plane (UP) for a Proxy Mobile IPv6 based network infrastructure. Existing specifications allow a MAG to perform splitting of its control and user plane using Alternate Care of address mobility option for IPv6, or Alternate IPv4 Care of Address option for IPv4. However, the current specification does not have semantics for allowing the LMA to perform such functional split. To realize this requirement, this specification defines a mobility option that enables a local mobility anchor to provide an alternate LMA address to be used for the bi-directional tunnel between the MAG and LMA. With this extension, a local mobility anchor will be able to use an IP address for its user plane which is different than what is used for the control plane.

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 January 17, 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. LMA User Plane Address Mobility Option	5
4. IANA Considerations	6
5. Security Considerations	6
6. Acknowledgements	6
7. References	6
7.1. Normative References	6
7.2. Informative References	6
Authors' Addresses	7

1. Introduction

Widely deployed mobility management systems for wireless communications have isolated the path for forwarding data packets from the control plane signaling for mobility management. To realize this requirement, Proxy Mobile IPv6 requires that the control plane functions of the local mobility anchor to be addressable at a different IP address than the IP address used for the user plane. However, the current specification does not have semantics for allowing the LMA to perform such functional split. The local mobility anchor is required to associate the IP address of the tunnel source with the target IP address of the control messages received from the MAG. Note that the concept of control- and user- planes are well established and understood in cellular networks.

A PMIPv6 infrastructure contains of two primary entities: MAG and LMA. The interface between MAG and LMA consists of two components: control plane and user plane. The control plane is responsible for signaling messages between MAG and LMA such as the Proxy Binding Update and Proxy Binding Acknowledge messages to establish a mobility binding. In addition, the control plane components in the MAG and LMA are also responsible for setting up and tearing down of the bi-directional tunnel between the MAG and LMA. The user plane is

responsible for forwarding the mobile node's IP packets between the MAG and the LMA over the bi-directional tunnel.

In most deployments, the control plane and user plane components (of the MAG and LMA) are co-located in the same physical entity. However, there are deployments where it is desirable to have the control and user plane of the MAG and LMA in separate physical entities. For example, in a WLAN (Wireless LAN) deployment, it may be desirable to have the control plane component of the MAG to be on Access Controller (also sometimes referred to as Wireless LAN Controller) while the user plane component of the MAG on the WLAN Access Point. This would enable all the signaling messages to the LMA to be centralized while the user plane would be distributed across the multiple Access Points. Similarly there is a case to split the control and user plane component of the LMA motivated by different scaling requirements on the control and user plane components or need to centralize the control plane in one geo-location while distributing the user plane component across multiple geo-locations

[RFC6463] and [RFC6275] contains a mechanism of splitting the control and user plane in MAG. Specifically, [RFC6463] defines an Alternate IPv4 Proxy Care of Address Option while [RFC6275] defines an Alternate Care of Address for IPv6 address. The MAG can provide an Alternate Care of Address in the Proxy Binding Update (PBU) and if the LMA supports this option then a bidirectional tunnel is setup between the LMA address and the MAG's alternate Care of address. However, there is no corresponding option for the LMA to provide an alternate address to the MAG.

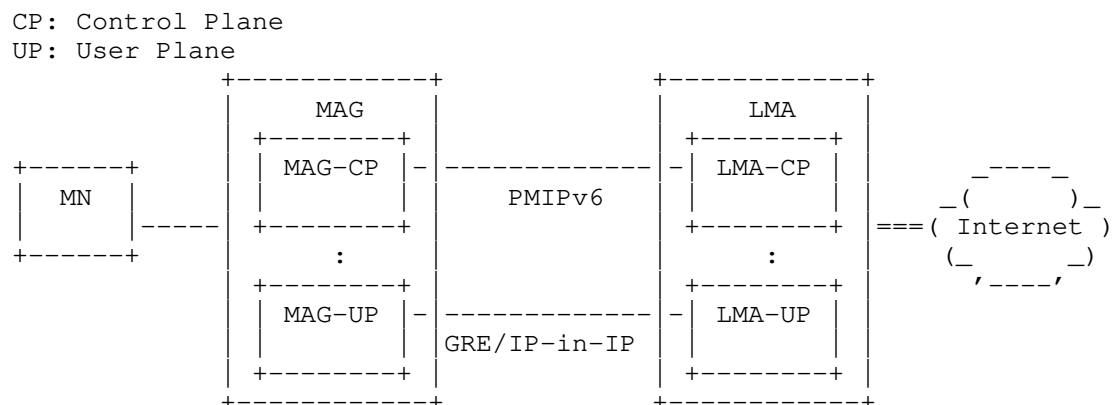


Figure 1: Functional Split of the Control and User Plane

This specification therefore defines a new mobility option that enables a local mobility anchor to provide an alternate LMA address to be used for the bi-directional tunnel between the MAG and LMA.

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]. 3GPP terms can be found at [RFC6459]. Additionally, this document uses the following terms:

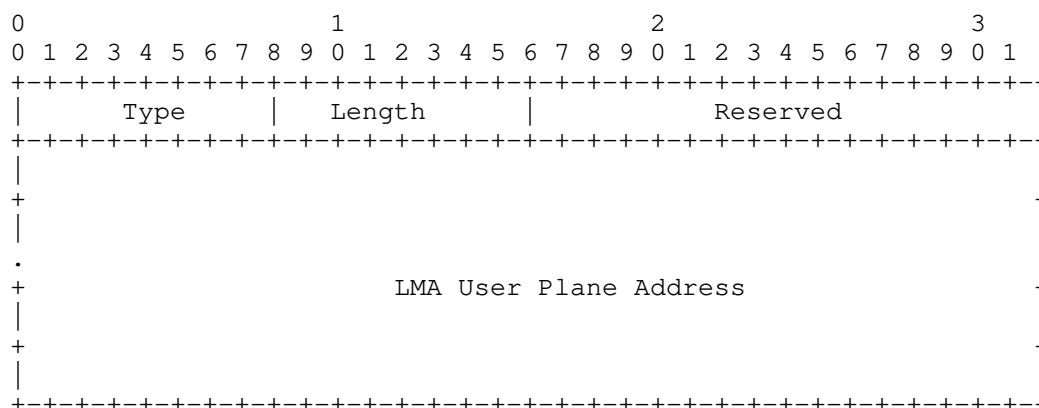
LMA User Plane Address (LMA-UPA)

The IP address on the LMA that is used for establishing tunnels with the mobile access gateway.

3. LMA User Plane Address Mobility Option

A new mobility header option, LMA User Plane Address mobility option is defined for use with Proxy Binding Acknowledgment message sent from the local mobility anchor to the mobile access gateway. This option is used for notifying the LMA's user plane IPv4/IPv6 address. There can be multiple instances of the LMA User Plane Address mobility option present in the message, one for IPv4 and the other for IPv6 transport.

The LMA User Plane Address mobility option has an alignment requirement of $8n+2$. Its format is as follows:



Type

To be assigned by IANA.

Length

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

Reserved

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

LMA User Plane Address

Contains the IPv4/IPv6 user plane address of the LMA.

4. IANA Considerations

This document requires the following IANA action.

- o Action-1: This specification defines a new Mobility Header option, LMA User Plane Address mobility option. This mobility option is described in Section 3. The type value <IANA-1> for this message needs to be allocated from the Mobility Header Types registry at <http://www.iana.org/assignments/mobility-parameters>. RFC Editor: Please replace <IANA-1> in Section 3 with the assigned value, and update this section accordingly.

5. Security Considerations

The LMA User Plane Address mobility Option defined in this specification is for use in Proxy Binding Acknowledgement message. This option is carried like any other mobility header option as specified in [RFC5213]. Therefore, it inherits from [RFC5213] its security guidelines and does not require any additional security considerations.

6. Acknowledgements

Authors would like Acknowledge all the discussions on this topic in the NETLMM Working group.

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

7.2. Informative References

- [RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
- [RFC6459] Korhonen, J., Soininen, J., Patil, B., Savolainen, T., Bajko, G., and K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459, January 2012.

[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

Ryuji Wakikawa
Softbank Mobile
1-9-1, Higashi-Shimbashi, Minato-Ku
Tokyo 105-7322
Japan

Email: ryuji.wakikawa@gmail.com

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

Email: rpazhyan@cisco.com

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

Email: sgundave@cisco.com