

NETEXT Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2011

CJ. Bernardos, Ed.
UC3M
March 14, 2011

Proxy Mobile IPv6 Extensions to Support Flow Mobility
draft-bernardos-netext-pmipv6-flowmob-03

Abstract

Proxy Mobile IPv6 (PMIPv6) is a network-based localized mobility management protocol that enables mobile devices to connect to a PMIPv6 domain and roam across gateways without changing their IP addresses. PMIPv6 basic specification also provides limited multi-homing support to multi-mode mobile devices. The ability of movement of selected flows from one access technology to another is missing in basic PMIPv6. This document describes enhancements to the Proxy Mobile IPv6 protocol that are required to support flow mobility over multiple physical interfaces.

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 15, 2011.

Copyright Notice

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

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

Table of Contents

1. Introduction	3
2. Terminology	3
3. Overview of the PMIPv6 flow mobility extensions	4
3.1. Use case scenarios	4
3.2. Basic Operation	5
4. Message formats	11
4.1. Flow Mobility Initiate (FMI)	11
4.2. Flow Mobility Acknowledge (FMA)	13
5. Conceptual Data Structures	14
5.1. Multiple Care-of Address Registration	14
5.2. Flow Mobility Cache	14
6. Mobile Node considerations	16
7. IANA Considerations	16
8. Security Considerations	16
9. Authors	16
10. Acknowledgments	18
11. References	18
11.1. Normative References	18
11.2. Informative References	18
Appendix A. Discussion items for IETF 80th	18
A.1. Summary of the ML discussion	19
A.2. Proposed changes for -04 version	19
Author's Address	20

1. Introduction

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

PMIPv6 allows an MN to connect to the same PMIPv6 domain through different interfaces. The "logical interface" at the IP layer may enable packet transmission and reception over different physical media. This technique can be used to achieve flow mobility, i.e., the movement of selected flows from one access technology to another. It is assumed that an IP layer interface can simultaneously and/or sequentially attach to multiple MAGs (possibly over multiple media). This document specifies protocol extensions to Proxy Mobile IPv6 between the LMA and MAGs for distributing specific traffic flows on different physical interfaces. This document assumes that a "logical interface" at the Mobile Node is capable of supporting traffic flows from different physical interfaces regardless of the assigned prefixes on those physical interfaces.

In particular, this document specifies how to manage "flow mobility" state in the PMIPv6 network (i.e. LMAs and MAGs), namely creation, refresh and cancel operation. Flow mobility is controlled by the LMA. The trigger causing the LMA to initiate a flow mobility operation is out of scope of this specification.

2. Terminology

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

FMI (Flow Mobility Initiate). Message sent by the LMA to create, refresh or cancel flow mobility state in the MAG. It conveys the information required to manage the flow mobility in a PMIPv6-Domain. This message is only needed when the flow mobility operation is not triggered by the attachment of a new interface of the mobile node.

FMA (Flow Mobility Acknowledge). Message sent by the MAG in reply to an FMI message. It provides feedback about the result of a flow mobility creation, refresh or cancel operation requested in the FMI message.

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

3. Overview of the PMIPv6 flow mobility extensions

3.1. Use case scenarios

Flow mobility assumes simultaneous access to more than one network, in a contrast to a typical handover where connectivity to a physical medium is relinquished, and is re-established with another. In order to support flow mobility in a PMIPv6 network, it is required to be able to tie the different PMIPv6 mobility sessions (one per interface) to a logical interface which is hiding one or more physical interfaces. The different mobility sessions in which a mobile node may be involved can share the same set of prefixes or have different ones:

1. 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 RFC 5213.
2. 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 in RFC 5213, and the LMA needs to be able to provide the same assignment even for the simultaneous attachment (as opposed to the handover

scenario only). It is assumed for the sake of this specification that the LMA has the knowledge if the MN supports the logical interface and if to assign the same prefix(es) or different prefix(es) to both access networks. How this is done is outside of the scope of this specification.

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

Among the above, scenario 2 MAY need extensions to RFC 5213 signaling at the time of a new attachment, 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 may be necessary between the LMA and the MAG.

The scenario 1 requires flow mobility signaling whenever the LMA determines the need for 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.

The scenario 3 requires flow mobility signaling whenever the LMA determines the need for relocating flows for the new prefix(es) which are not shared across attachments.

In all the scenarios, the MAGs should be aware of the prefixes for which the MN is going to receive traffic. As a result of a flow mobility operation, these prefixes might not be limited to those delegated by the MAG upon attachment of the connected interface, and therefore in these cases, signaling is required.

The extensions described in this document support any of these aforementioned scenarios.

3.2. Basic Operation

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

When a multi-interfaced mobile node connects to a PMIPv6-domain, it performs regular attachment and as a result is able to configure an IP address (or a set of IP addresses) on the logical interface hiding the different physical interfaces. If the LMA assigns a common prefix (or set of prefixes) to the different physical interfaces attached to the domain, then all the MAGs have already all the

routing knowledge required to forward packets to the mobile node, and the LMA does not need to perform any kind of signaling in order to move flows across the different physical interfaces. Note that there should be a local policy in place that ensures that the mobile node sends outbound packets using the same physical interface from which packets belonging to the same flow are being received (the used interface might change during the lifetime of a communication). This SHOULD be enforced by the logical interface engine, and the details about how this is done are out of the scope of this document). For unidirectional outbound communications, there SHOULD be a policy at the mobile node defining which physical interface is used to send the traffic. For bidirectional outbound communications, there SHOULD be also such a policy, but its content must be consistent with the policy at the network-side (the details about how this consistency is ensured are out of the scope of this document).

In case the MAGs needs to be informed about flow mobility decisions, because of packet policing, packet enforcement, charging or similar reasons, the LMA MAY re-use the signaling defined later in this document to convey this information.

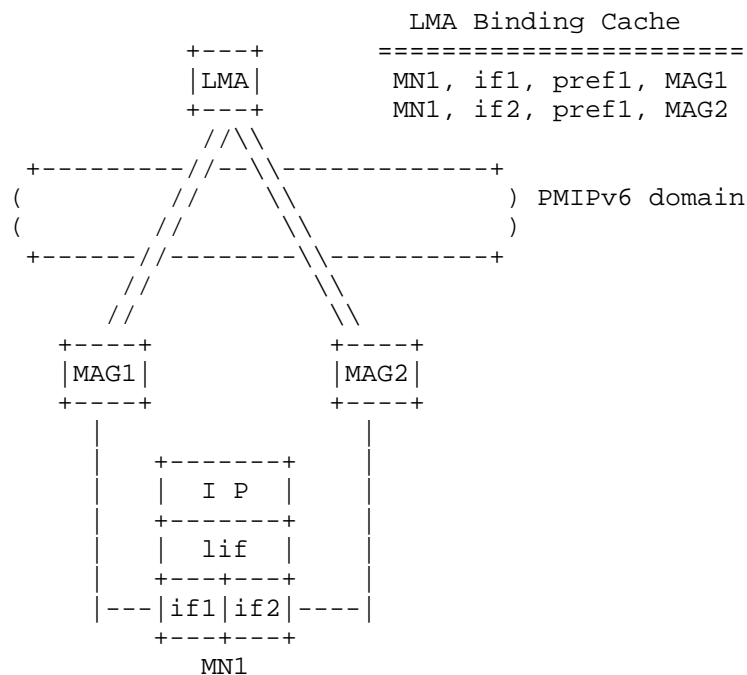


Figure 1: Shared prefix across physical interfaces scenario

Next, an example of how flow mobility works in this case is shown.

In Figure 1, a mobile node (MN1) has two different physical interfaces (if1 and if2), grouped in a unique logical interface (lif). Each physical interface is attached to a different MAG, both of them anchored and controlled by the same LMA. Since both physical interfaces are assigned the same prefix (pref1) upon attachment to the MAGs, the mobile node has one single IPv6 addresses configured on the logical interface: pref1::lif. Initially, flow X goes through MAG1 and flow Y through MAG2. The LMA, at a certain point, decides to move flow Y, so it also goes through MAG1. As show in Figure 2, no signaling between the LMA and the MAGs is needed.

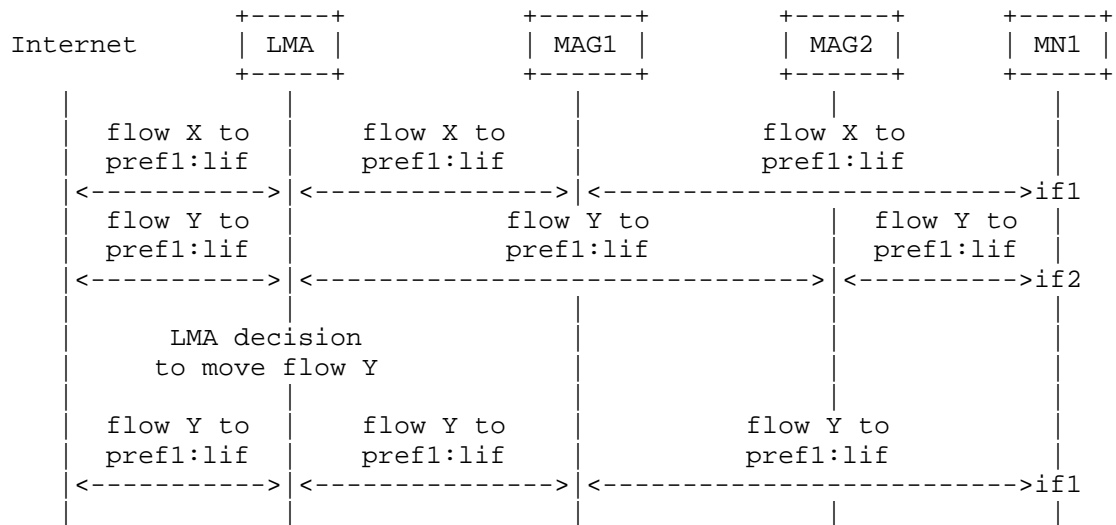


Figure 2: Flow mobility message sequence when the LMA assigns a common set of prefixes

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

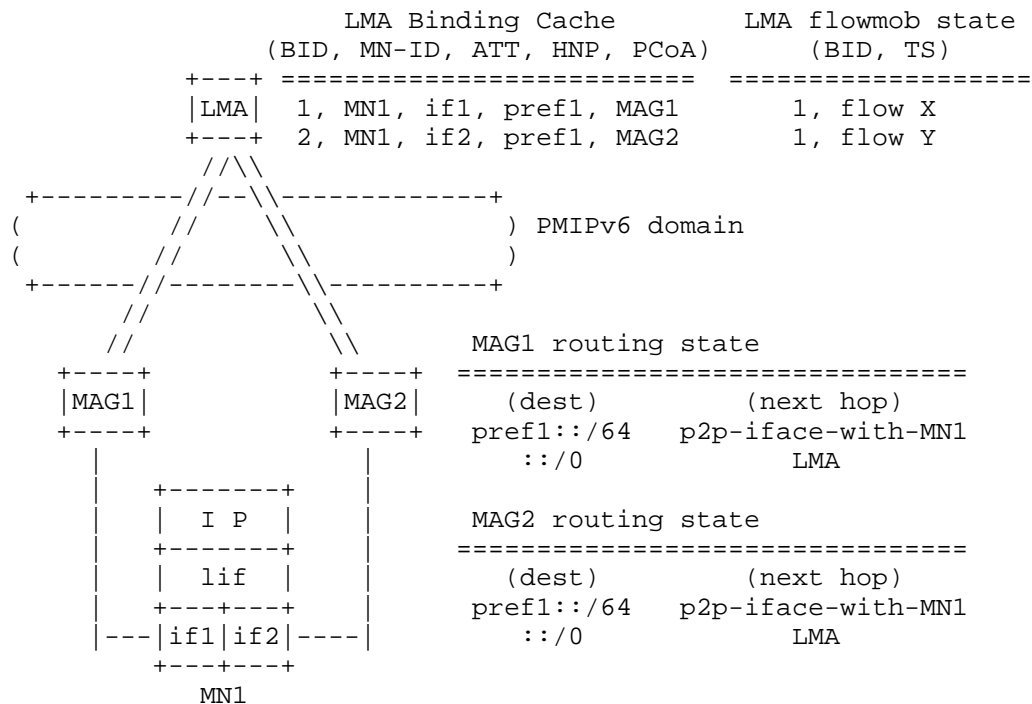


Figure 3: Data structures when the LMA assigns a common set of prefixes

A different flow mobility scenario happens when the LMA assigns different set of prefixes to physical interfaces of the same mobile node. In this case specific signaling is required between the LMA and the MAG to support this scenario. Two different possibilities are considered next.

One first possible case is the following (shown in Figure 4). The mobile node is already attached to the PMIPv6-Domain via MAG1. At a certain moment, the mobile node attaches a new interface (if2) to MAG2. MAG2 sends a PBU which is then used as a trigger by the LMA to decide perform a flow mobility decision. In this case, we consider that flows are moved with a prefix granularity, meaning that the LMA moves flows by moving prefixes among the different MAGs the mobile node is attached to. In this example, flow Y is bound to pref2::/64 and therefore the LMA can move the flow by just binding pref2::/64 to MAG2. This is done by including the prefix in the PBA message, and optionally sending a message to MAG1 to remove the transferred prefix(es). This message can be a Binding Revocation Indication message [RFC5846] with the P bit set to indicate that this is revocation of PMIP prefix(es). After processing BRI, the source MAG

will send a Binding Revocation Acknowledgement (BRA) message back to LMA.

Note that this specification also supports flow mobility at a finer granularity (not just on a prefix level). This is done by including in the PBA a Flow Identification Mobility option (specified in [RFC6089]) which can convey full flow information. The MAG can also include the Flow Identification Mobility option in the PBU message that it sends to the LMA. This serves as a request for the LMA to consider the flow policy rules specified in the option.

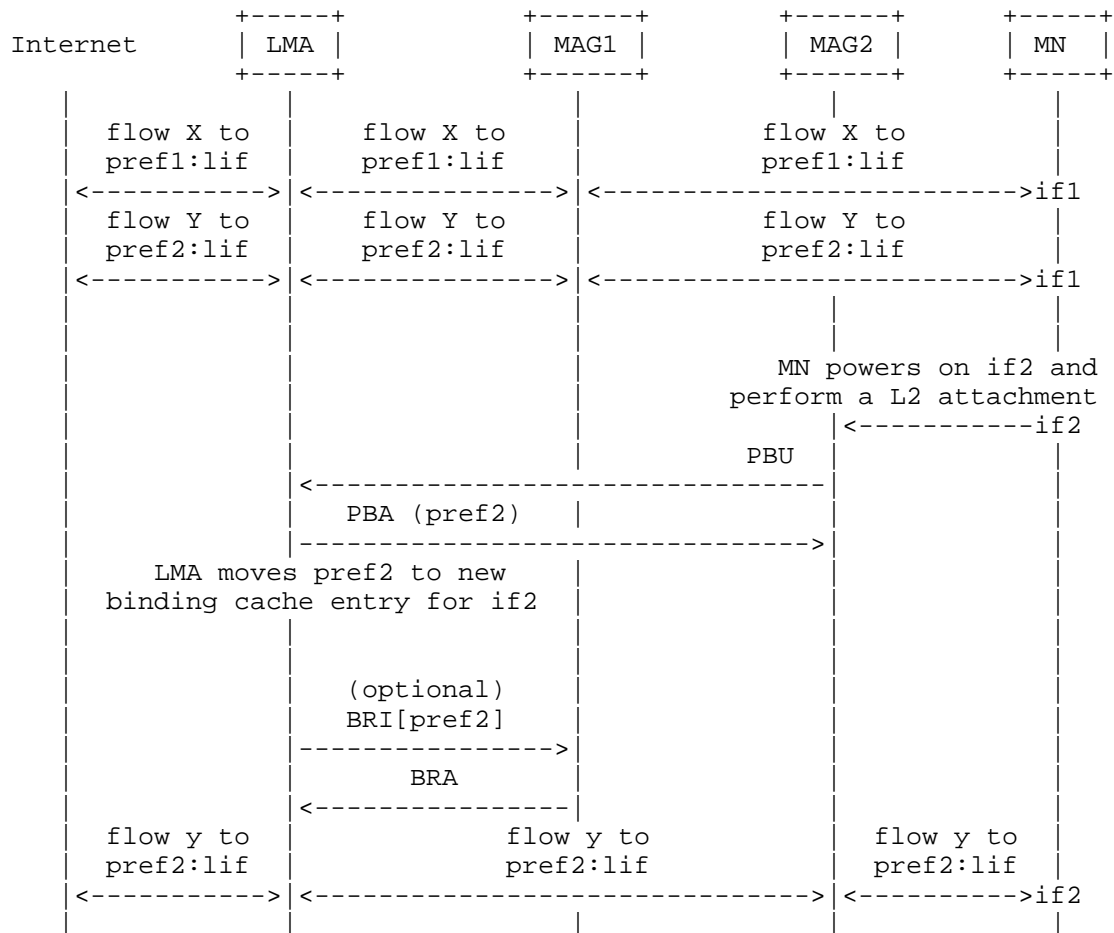


Figure 4: Flow mobility message sequence when the LMA assigns different set of prefixes per physical interface (PBU trigger)

A second possible scenario is the following. A multi-interfaced

mobile node is attached to a PMIPv6-Domain and the LMA, at a given moment, decides to move a flow. The LMA can decide to move a flow as a result of a policy change or upon receiving a trigger either based on network status or based on an event detected at the mobile node and transported via old or new MAG. How this decision is taken is out of scope of this specification. Since the LMA cannot send a PBA message which has not been triggered in response to a received PBU message, new signaling messages are defined to cover this case.

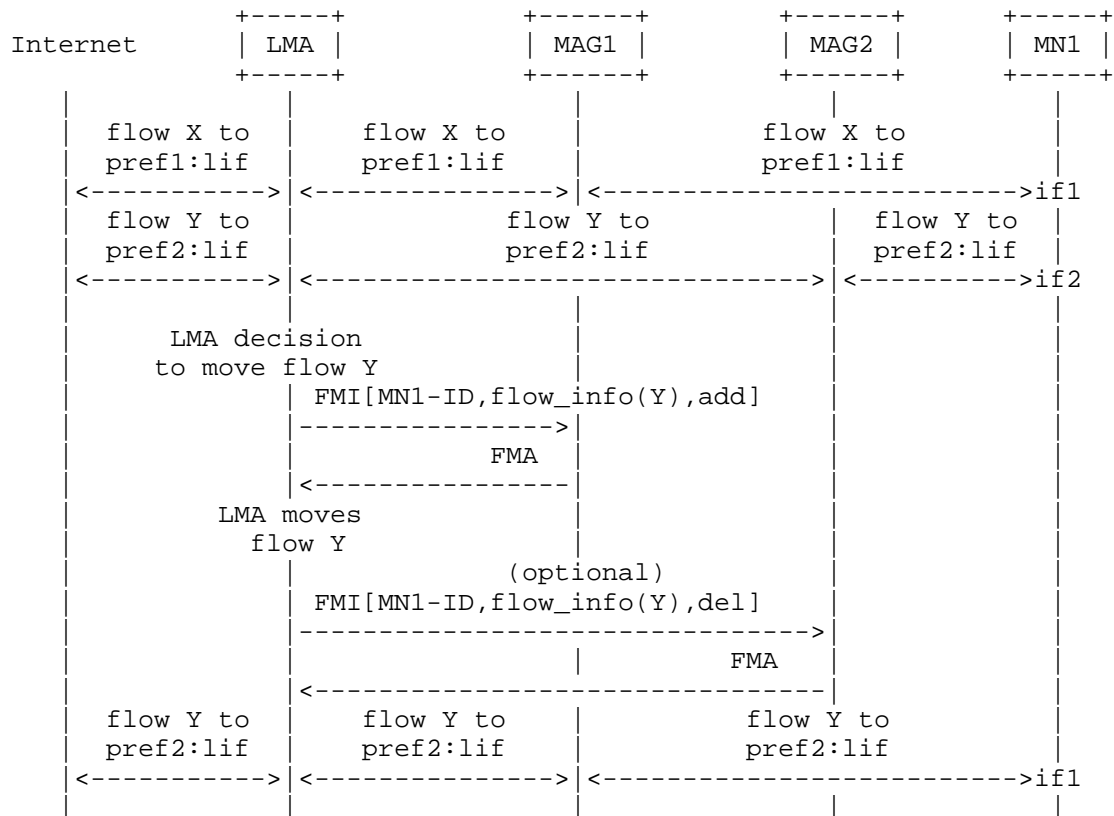


Figure 5: Flow mobility message sequence when the LMA assigns different set of prefixes per physical interface (FMI trigger)

If the LMA decides to move a particular flow from its default path (which is determined by the destination prefix) to a different one, it constructs a Flow Mobility Initiate (FMI) message. This message is sent to the new target MAG, i.e. the one selected to be the used in the forwarding of the flow. The FMI message contains (as explained in further detail in Section 4.1), the MN-Identifier, the Flow Identification Mobility option (specified in [RFC6089]) which

can convey prefix or full flow information, and the type of flow mobility operation (add flow). Optionally, the LMA may send another FMI message, this time to remove the flow Y state at MAG2. Otherwise the flow state at MAG2 will be removed upon timer expiration. The message sequence is shown in Figure 5.

The state in the network after moving a flow, for the case the LMA assigns a different set of prefixes is shown in Figure 6.

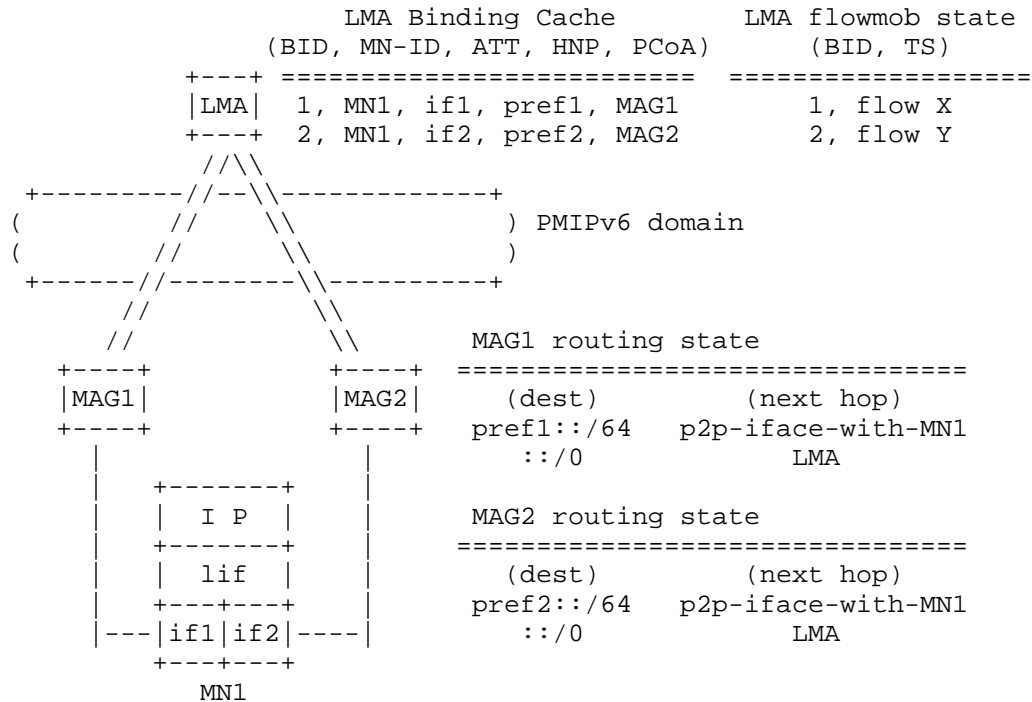
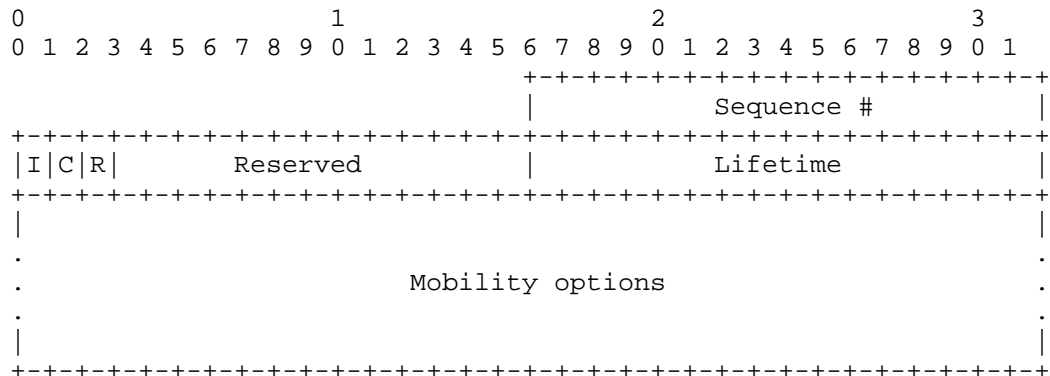


Figure 6: Data structures when the LMA assigns a different set of prefixes

4. Message formats

4.1. Flow Mobility Initiate (FMI)

The LMA sends an FMI message to a MAG to inform about a particular flow movement (LMA initiated). It is a Mobility Header message.

**Sequence Number:**

A monotonically increasing integer. Set by the LMA sending then initiate message, and used to match a reply in the acknowledge.

'I' (initiate) flag:

Set to 1, indicates it is an FMI message.

'C' (cancel) flag:

When set to 1, indicates a request to remove state about the flow (cancel flow mobility). If set to 1, the Lifetime field MUST be set to 0.

'R' (refresh) flag:

When set to 1, indicates a request to refresh state about the flow. If the 'C' flag is set to 1, this flag should be set to 0 by the sender and ignored by the receiver.

Reserved:

This field is unused. MUST be set to zero by the sender.

Lifetime:

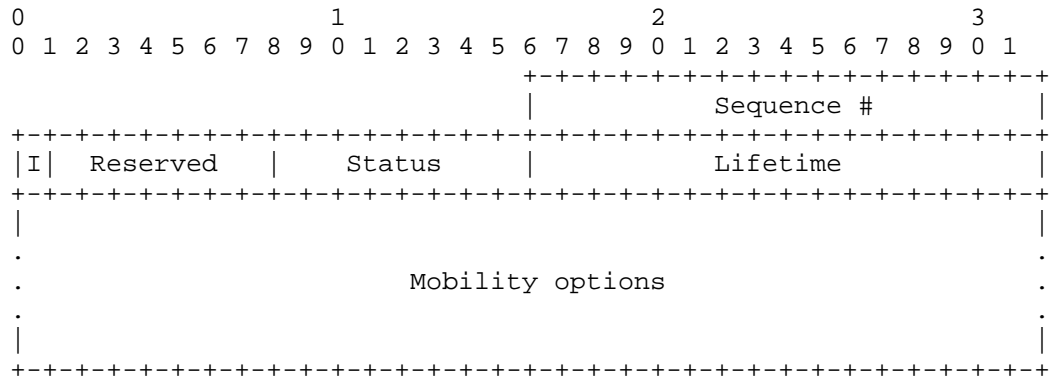
The requested time in seconds for which the LMA asks the MAG keep flow-specific state. A value of all one bits (0xffff) represents infinity.

Mobility Options:

MUST contain the MN-ID, followed by one or more Flow Identification Mobility options [RFC6089].

4.2. Flow Mobility Acknowledge (FMA)

The MAG sends an FMI message to the LMA as a response to the FMI message. It is a Mobility Header message.



Sequence Number:

A monotonically increasing integer. Copied from the value set by the sending LMA in the FMI message being acknowledged by this FMA message.

'I' flag:

Set to 0, indicates it is an FMA message.

Reserved:

This field is unused. MUST be set to zero by the sender.

Status:

0: Success.

128: Reason unspecified.

129: MN not attached.

130: Sequence number out of window.

131: Traffic Selector format unsupported.

132: No existing Flow Mobility Cache entry.

133: Already existing Flow Mobility Cache entry.

Lifetime:

The requested time in seconds for which the MAG keeps flow-specific state. A value of all one bits (0xffff) represents infinity.

Mobility Options:

When Status code is 0, MUST contain the MN-ID, followed by one or more Flow Identification Mobility options [RFC6089].

5. Conceptual Data Structures

5.1. Multiple Care-of Address Registration

The LMA is extended to allow a mobile node to register multiple proxy care of address (Proxy-CoA). The LMA maintains multiple binding cache entries for a MN. The number of binding cache entries of a MN is equal to the number of the MN's interfaces attaching to the MAG.

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

Figure 7: Extended Binding Cache

Figure 7 shows two Binding Cache Entries of the MN1 when it attaches to the network using two different access technologies. Both of the two attachments share HNP1 and are bounded to two different Proxy-CoAs.

5.2. Flow Mobility Cache

Each LMA must maintain a flow mobility cache (FMC) as shown in Figure 8. This table contains entry for each flow sent from the MN. A flow binding entry includes the following fields:

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

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

Figure 8: Flow Mobility Cache

The BIDs field contains the identifier of the binding cache entry that all of the packets matching the flow information described in the TS field will be forwarded to. When the flow mobility occurs, the BIDs will be updated with new binding cache entry identifier.

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

The Mobile Access Gateway MAY also maintain a similar data structure. In case no full flow mobility state is required at the MAG, the Binding Update List (BUL) data structure is enough and no extra conceptual data entries are needed. In case full per-flow state is required at the MAG, it should keep a similar structure to the FMC (details TBD).

6. Mobile Node considerations

This specification assumes the MN implements the logical interface model. The "logical interface" at the IP layer hides the use of different physical media from the IP stack, enabling the MN to send and receive packets over different interfaces. This document assumes the MN behaves as stated in the applicability statement document [I-D.ietf-netext-logical-interface-support]. In particular, it is assumed that -- for the case of bidirectional traffic -- the logical interface at the MN "replicates" the behavior observed for downlink packets on a per-flow basis. This means that the MN sends UL Flow X on the same interface which received the DL Flow X. It also means that if the LMA moves flow X during its lifetime, the MN will follow that change, upon the reception of packets of flow X via a different interface.

This specification only supports flow mobility between different physical interfaces belonging to the same logical interface. If an MN has several logical interfaces, flow mobility across different logical interfaces is not supported.

7. IANA Considerations

TBD.

8. Security Considerations

TBD.

9. Authors

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

Kuntal Chowdhury

E-mail: Kchowdhu@cisco.com

Vijay Devarapalli

E-mail: vijay@wichorus.com

Sri Gundavelli

E-mail: sgundave@cisco.com

Youn-Hee Han

E-mail: yhhan@kut.ac.kr

Yong-Geun Hong

E-mail: yonggeun.hong@gmail.com

Mohana Dahamayanthi Jeyatharan

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

Rajeev Koodli

E-mail: rkoodli@cisco.com

Kent Leung

E-mail: kleung@cisco.com

Telemaco Melia

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

Bruno Mongazon-Cazavet

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

Chan-Wah Ng

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

Behcet Sarikaya

E-mail: sarikaya@ieee.org

Tran Minh Trung

E-mail: trungtm2909@gmail.com

Frank Xia

E-mail: xiayangsong@huawei.com

10. Acknowledgments

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

11. References

11.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5846] Muhanna, A., Khalil, M., Gundavelli, S., Chowdhury, K., and P. Yegani, "Binding Revocation for IPv6 Mobility", RFC 5846, June 2010.
- [RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, January 2011.
- [RFC6089] Tsirtsis, G., Soliman, H., Montavont, N., Giaretta, G., and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support", RFC 6089, January 2011.

11.2. Informative References

- [I-D.ietf-netext-logical-interface-support] Melia, T. and S. Gundavelli, "Logical Interface Support for multi-mode IP Hosts", draft-ietf-netext-logical-interface-support-01 (work in progress), October 2010.

Appendix A. Discussion items for IETF 80th

This appendix tries to serve as basis for the discussion in the IETF 80th on flow mobility. It includes a summary of the major issues/comments raised on the NETEXT mailing list, as well as a proposed plan for a future revision of the document.

A.1. Summary of the ML discussion

Here we list (in no particular order) some of the issues raised on the NETEXT mailing list:

- o Lack of realistic scenario for applicability: no use-case/client for LMA-initiated mobility, no real-life scenario where the LMA would receive flow mobility policies.
- o Consistency of policy rules between the MN and LMA does not ensure that the LMA knows what decision the MN took because the LMA does not necessarily know the context in which the MN is.
- o Discrepancies on the solution approach: dynamic attachment/detachment of interfaces from sessions (new prefixes cannot be added to sessions) vs dynamic prefix management. It's being argued that the draft changes the basics of RFC5213 session management.
- o Discrepancies on the solution approach: requirement on the existence of L2 triggers to aid in the dynamic attachment/detachment of interfaces from sessions for flow mobility purposes.
- o How does the LMA know channel condition of each radio, applications requirements of apps running in the UE?.
- o Source of triggers for flow mobility: MAG, LMA or both?

A.2. Proposed changes for -04 version

Based on the discussion on the ML list, a possible way to modify this document in -04 version is the following. We define two different approaches, based on the L2 signaling support:

1. L2 signaling based. When an MN attaches to a new MAG, it can use extended L2 signaling (e.g., HI=FM) to indicate that the attachment is for flow mobility. In this case, same prefix is assigned to the new interface (which is added to the existing mobility session). Alternatively, a new prefix can also be added to the session (this is up to the policy configured). Now new signaling is required between MAG and LMA, just a new HI value, the extended L2 signaling in place and updating the state machines of MAG and LMA to support this new behavior.
2. IP based. If no extended L2 signaling is available (i.e., no HI=FM), MAGs create new sessions upon new MN interface attachment. The LMA manages the prefixes of the session (decides

to assign the same of an already attached interface or a new one) as well as the movement of them (with a prefix/flow granularity). The trigger for the movement of a flow is out of scope (MAG triggers are considered). This is basically the operation described in the current version of the draft.

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/>

NETEXT WG
Internet-Draft
Intended status: Standards Track
Expires: January 4, 2012

S. Gundavelli
Cisco
J. Korhonen
Nokia Siemens Networks
M. Grayson
K. Leung
Cisco
July 3, 2011

Access Network Information Option for Proxy Mobile IPv6
draft-gundavelli-netext-access-network-option-01.txt

Abstract

This specification defines a mechanism and a related mobility option for carrying the access network identifier and the access operator identification information from the mobile access gateway to the local mobility anchor over Proxy Mobile IPv6. Based on the received information, the local mobility anchor is able to provide access network and access operator specific handling or policing for the mobile node traffic.

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 4, 2012.

Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Conventions and Terminology	4
2.1. Conventions	4
2.2. Terminology	4
3. Protocol Considerations	4
4. Access Network Identifier Option	5
5. IANA Considerations	7
6. Security Considerations	7
7. Acknowledgements	8
8. References	8
8.1. Normative References	8
8.2. Informative References	8
Authors' Addresses	8

1. Introduction

In many deployments there is a need for the local mobility anchor to provide differentiated services and policing to the mobile nodes based on the access network to which they are attached. Policy systems in mobility architectures such as PCC [TS23203] and ANDSF [TS23402] in 3GPP system allow configuration of policy rules with conditions based on the access network information. For example, the service treatment for the mobile node's traffic may be different when they are attached to a access network owned by the home operator than when owned by a roaming partner. The service treatment can also be different based on the configured SSID in case of IEEE 802.11 based access networks.

The Proxy Mobile IPv6 specification [RFC5213] allows carrying of the Access Technology Type (ATT) information from the mobile access gateway to the local mobility anchor. However, the Access Technology Type alone is not sufficient for correct policy to be applied at the LMA and there is a need to ensure additional information related to the access network is available. Learning the access network operator identity may not be possible for an LMA without a support of an additional policy framework that is able to provide required information out of band to the LMA. Such a policy framework may not be required for all Proxy Mobile IPv6 deployments and hence an alternative approach for carrying such information is required to ensure that additional information related to the access network is available.

This document defines a new mobility option, Access Network Identifier (ANI) option for Proxy Mobile IPv6 (PMIPv6), that can be used by mobile access gateway (MAG) for carrying the access network information to the local mobility anchor. The specific details on how the local mobility anchor uses this information is out-of-scope for this document.

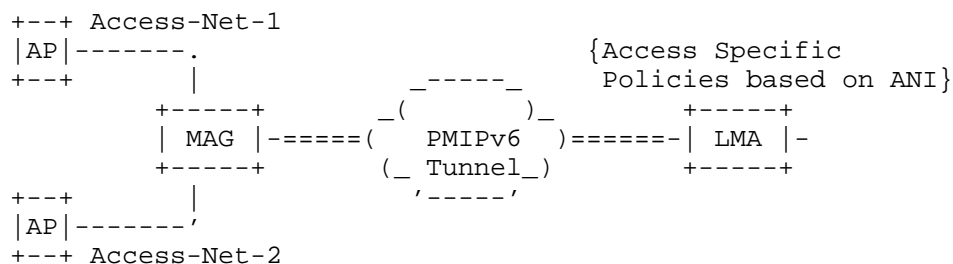


Figure 1: Access Networks attached to MAG

Figure 1, illustrates the scenario where the IEEE 802.11 Access Points are configured to the mobile access gateway.

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] and [RFC5844]. Additionally, this document uses the following abbreviations:

ANDSF

Access Network Discovery and Selection Framework

PCC

Policy and Charging Control Framework

Service Set Identifier

Service Set Identifier (SSID) identifies the name of the IEEE 802.11 network. SSID differentiates from one network to the other.

Vendor ID

The Vendor ID is the SMI Network Management Private Enterprise Code of the IANA-maintained Private Enterprise Numbers registry [SMI].

3. Protocol Considerations

The following considerations apply to the local mobility anchor and the mobile access gateway.

- o 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 access network information

associated with the current session. Specifically, the following parameters must be defined.

Network Identifier

Operator Identifier

- o 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 access network information associated with the current session. Specifically, the following parameters must be defined.

Network Identifier

Operator Identifier

- o The mobile access gateway may be statically configured with the access network information related to the access links its attached to. In access systems where the mobile access gateway is attached to a micro-mobility domain such as IEEE 802.11 WLAN domain, the DHCP relay agent function in that micro-mobility domain may be configured to add the access network information in DHCP option (82), which is the DHCP Relay Agent Information option [RFC3046]. The mobile access gateway may learn the access network information from this option.
- o On receiving a Proxy Binding Update message [RFC5213] from a mobile access gateway with the Access Network Information option, the local mobility anchor must process the option and update the corresponding fields in the Binding Cache entry.
- o The local mobility anchor MAY choose to use the access network information options for applying any access operator specific handling or policing of the mobile node traffic.

4. Access Network Identifier Option

A new option, Access Network Information option, is defined for using it in Proxy Binding Update (PBU) and Proxy Binding Acknowledgement (PBA) messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for carrying the information related to the access network to which the mobile node is attached.

The alignment requirement for this option is 4n.

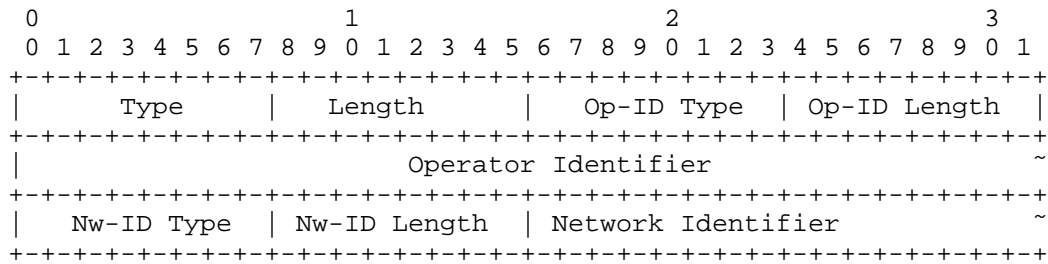


Figure 2: Access Network Identifier Option

Type

TBD by IANA

Length

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

Op-ID Type

8-bit unsigned integer indicating the type of the Operator Identifier. Currently the following types are defined:

1. reserved.
2. Vendor ID as a Private Enterprise Number [SMI].
3. Realm of the operator. Realm names are required to be unique, and are piggybacked on the administration of the DNS namespace.

Op-ID Length

8-bit unsigned integer indicating the number of octets-1 needed to encode the Operator Identifier.

Operator Identifier

Up to 256 octets of the operator identifier. The encoding of the identifier depends on the used OP-ID Type.

Nw-ID Type

8-bit unsigned integer indicating the type of the Network Identifier. Currently the following types are defined:

1. reserved.
2. SSID of the IEEE 802.11 network.
3. Geolocation of the Access Point

Nw-ID Length

8-bit unsigned integer indicating the number of octets-1 needed to encode the Network Identifier.

Network Identifier

Up to 256 octets of the network identifier. The encoding of the identifier depends on the used Nw-ID Type.

5. IANA Considerations

This specification defines a new Mobility Header option, the Access Network Information. This option is described in Section 4. The Type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options, as defined in [RFC3775].

Furthermore, this specification creates a two new name spaces: Op-ID Type ND Nw-ID Type. Both are described with their initial allocations in Section 4. These two name spaces are placed under the Mobile IPv6 parameters registry for [RFC3775].

6. Security Considerations

The Access Network Information 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 [RFC3775] and does not require any special security considerations.

The Access Technology Type option [RFC5213] is always present in the Proxy Binding Update and Proxy Binding Acknowledgement messages. Carrying additional details related to the access network to which the mobile node is attached does not introduce any new security

vulnerabilities.

7. Acknowledgements

The authors would also like to acknowledge all the discussions related to carrying Access Network Information option in Proxy Mobile IPv6 protocol signaling. Additionally, the authors would like to thank Stefano Faccin, Gerardo Gieratta, Rajesh Pazhyannur, and Eric Voit for all the discussions around this topic.

8. References

8.1. 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.

8.2. Informative References

- [RFC3046] Patrick, M., "DHCP Relay Agent Information Option", RFC 3046, January 2001.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [SMI] IANA, "PRIVATE ENTERPRISE NUMBERS", SMI Network Management Private Enterprise Codes, February 2011.
- [TS23203] 3GPP, "Policy and Charging Control Architecture", 2010.
- [TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 2010.

Authors' Addresses

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

Email: sgundave@cisco.com

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

Email: jouni.nospam@gmail.com

Mark Grayson
Cisco
11 New Square Park
Bedfont Lakes, FELTHAM TW14 8HA
ENGLAND

Email: mgrayson@cisco.com

Kent Leung
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: kleung@cisco.com

NETEXT WG
Internet-Draft
Intended status: Standards Track
Expires: January 6, 2012

S. Gundavelli, Ed.
Cisco
X. Zhou
ZTE Corporation
J. Korhonen
Nokia Siemens Networks
G. Feige
R. Koodli
Cisco
July 5, 2011

IP Traffic Offload Selector Option for Proxy Mobile IPv6
draft-gundavelli-netext-pmipv6-sipto-option-01.txt

Abstract

This specification defines a mechanism and a related mobility option for carrying IP Offload traffic selectors between a mobile access gateway and a local mobility anchor in a Proxy Mobile IPv6 domain. Based on the received offload flow selectors from the local mobility anchor, a mobile access gateway can enable offload traffic rule on the selected IP flows.

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 6, 2012.

Copyright Notice

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

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

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

Table of Contents

1. Introduction	3
2. Conventions and Terminology	3
2.1. Conventions	4
2.2. Terminology	4
3. Solution Overview	4
3.1. LMA Considerations	5
3.2. MAG Considerations	6
4. IP Traffic Offload Selector Option	6
5. IANA Considerations	7
6. Security Considerations	8
7. Acknowledgements	8
8. References	8
8.1. Normative References	8
8.2. Informative References	9
Authors' Addresses	9

1. Introduction

Mobile Operators are expanding their network coverage by integrating various access technology domains into a common IP mobile core. For providing IP mobility support to a mobile node irrespective of the access network to which it is attached, the 3GPP S2/a Proxy Mobile IPv6 [TS23402] interface, specified by the 3GPP system architecture, is providing the needed protocol glue. When this protocol interface based on Proxy Mobile IPv6 [RFC5213] is used, the mobile node is topologically anchored on the local mobility anchor [RFC5213] in the home network. The mobile node's IP traffic is always tunneled back from the mobile access gateway [RFC5213] in the access network to the local mobility anchor in the home network.

However, with the exponential growth in the mobile data traffic, mobile operators are exploring new ways to offload some of the IP traffic flows at the nearest access edge where ever there is an internet peering point, as supposed to carrying it all the way to the mobility anchor in the home network. Not all IP traffic needs to be routed back to the home network, some of the non-essential traffic which does not require IP mobility support can be offloaded at the mobile access gateway in the access network. This approach provides greater leverage and efficient usage of the mobile packet core with increased overall network capacity and by lowering transport costs. The local mobility anchor in the home network can potentially deliver the IP flow selectors to the mobile access gateway in the access network, for identifying the IP flows that needs to be offloaded.

This document defines a new mobility option, IP Traffic Offload Selector option for Proxy Mobile IPv6 (PMIPv6). This option can be used by the local mobility anchor for notifying the flow selectors for that can be used by the local mobility anchor for notifying the mobile access gateway flows that can be offloaded at the access edge. Since, the mobile node's IP address topologically belongs to the home network, the offloaded IP traffic flows need to be NAT [RFC2663] translated. Given this NAT translation requirement for the offloaded traffic, this approach will be limited to mobile node's IPv4 flows. There are better ways to solve this problem for IPv6 and with the goal not to create NAT66 requirement, this specification does not support traffic offload support for IPv6 flows. This document also does not define any new semantics for flow selectors. The flow identification and the related semantics are all leveraged from [RFC6088].

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

IP Flow

IP Flow represents a set of IP packets that match a traffic selector. The selector is typically based on the source IP address, destination IP address, source port, destination port and other fields in upper layer headers.

Selective IP Traffic Offload (SIPTO)

Ability to select specific IP flows and route them to the local network, as supposed to tunneling them to the home network.

NAT (Network Address Translation)

Network Address Translation [RFC2663] is a method by which IP addresses are mapped from one address realm to another, providing transparent routing to end hosts.

3. Solution Overview

The following illustrates the scenario where the mobile access gateway in an access network having the ability to offload some of the IPv4 traffic flows, based on the traffic selectors it received from the local mobility anchor in the home network.

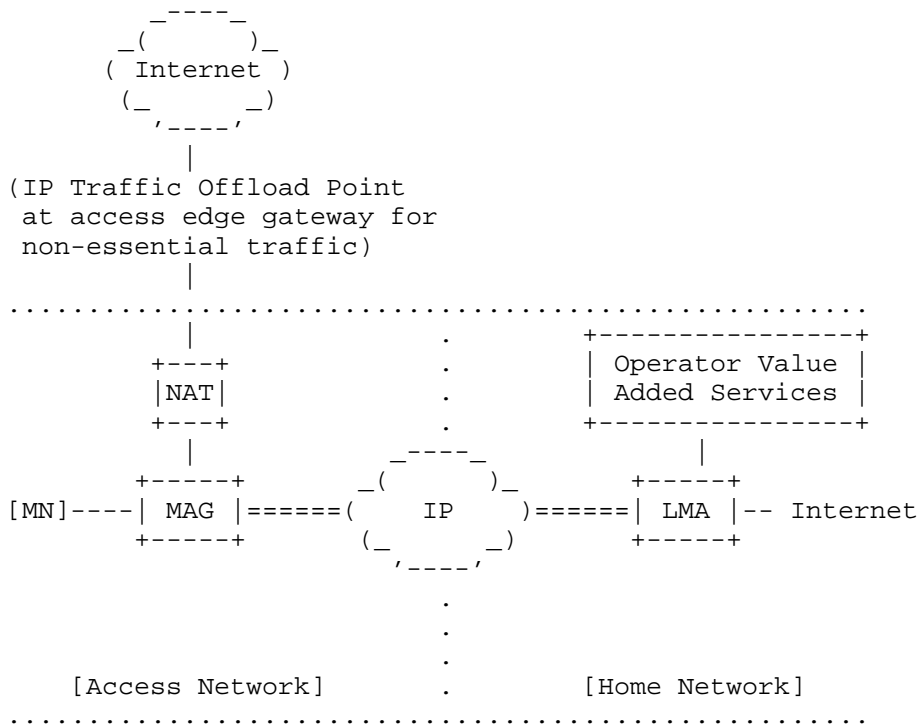


Figure 1: Access Networks attached to MAG

3.1. LMA Considerations

The following considerations apply to the local mobility anchor and the mobile access gateway.

Figure 1 explains the operational sequence of the IP Traffic Offload selectors between the mobile access gateway and the local mobility anchor.

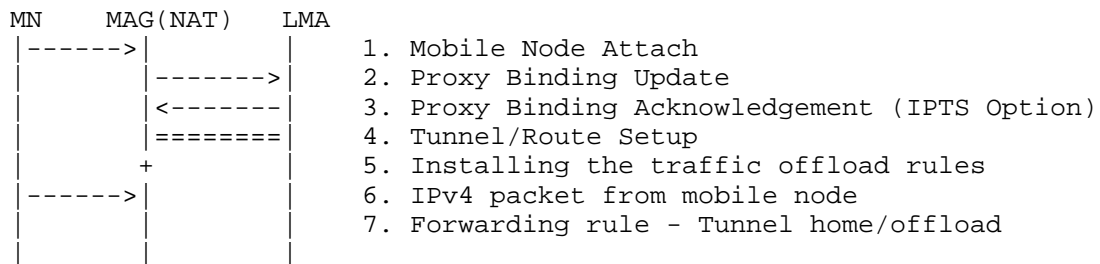


Figure 2: Exchange of IP Traffic Offload Selectors

- o If the received Proxy Binding Update includes the IP Traffic Offload Selector Option Section 4, but if the local mobility anchor either does not have the SIPTO capability, or it chooses to deny the SIPTO request, the local mobility anchor MUST ignore the IP Traffic Offload Selector Option and this would have no effect on the operation of the rest of the protocol.
- o If the local mobility anchor has the SIPTO capability and chooses to deliver the flow policies, the local mobility anchor can construct the traffic selectors based on the routing policy and deliver those selectors in the Proxy Binding Acknowledgement message using the IP Traffic Offload Selector Option. If the received Proxy Binding Update included a proposed Offload traffic selectors, the local mobility anchor MAY choose to honor that request.

3.2. MAG Considerations

- o The mobile access gateway MAY choose to notify the local mobility anchor about its SIPTO capability by including the IP Traffic Offload Selector Option Section 4 in the Proxy Binding Update message. The included option MAY include the proposed offload selectors which the local mobility anchor may choose to override. If the mobile access gateway cannot does not have SIPTO capability, this option MUST NOT be included in the Proxy Binding Update.
- o If there is no IP Traffic Offload Selector Option in the corresponding Proxy Binding Acknowledgement message, it is considered that the local mobility anchor does not support SIPTO capability, specifically, it cannot deliver selectors for IP traffic offload flows.
- o If there IP Traffic Offload Selector Option in the corresponding Proxy Binding Acknowledgement message, it serves as an hint that the local mobility anchor can support SIPTO and the included traffic spec MUST be applied by the mobile access gateway.

4. IP Traffic Offload Selector Option

A new option, IP Traffic Offload Selector option, is defined for using it in Proxy Binding Update (PBU) and Proxy Binding Acknowledgement (PBA) messages exchanged between a local mobility anchor and a mobile access gateway. This option is used for carrying the flow selectors for supporting IP traffic offload function at the

mobile access gateway. The option includes the parameters for selecting IP flows for offload.

The alignment requirement for this option is 4n.

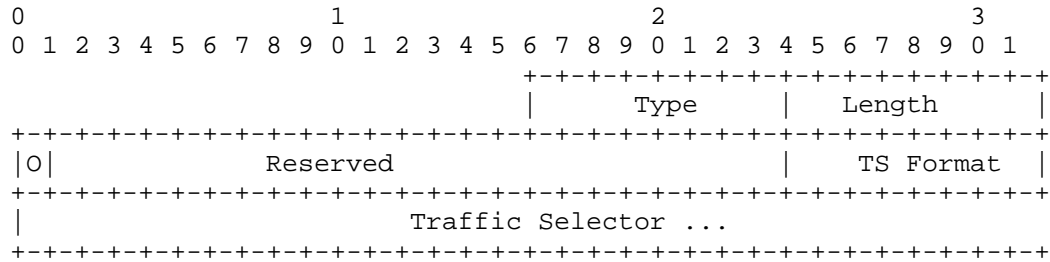


Figure 3: IP Traffic Offload Selector Option

Type

<IANA>

Length

8-bit unsigned integer indicating the length in octets of the option, 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.

TS Format An 8-bit unsigned integer indicating the Traffic Selector Format. Value "0" is reserved and MUST NOT be used. The value of (1) is assigned for IPv4 Binary Traffic Selector [RFC6088].

TS Selector A variable-length opaque field for including the traffic specification identified by the TS format field. When the value of TS Format field is set to (1), the format that follows is the IPv4 Binary Traffic Selector specified in section 3.1 of [RFC6088].

5. IANA Considerations

This document requires the following two IANA actions.

- o Action-1: This specification defines a new Mobility Header option, IP Traffic Offload Selector option. This option is described in Section 4. The Type value for this option needs to be assigned

from the same numbering space as allocated for the other mobility options [RFC3775].

- o Action-2: The Sub-type field of the IP Traffic Offload Selector option introduces a new number space. This number space needs to be managed by IANA, under the Registry, IP Traffic Offload Selector Type Registry. This specification reserves the sub-type value of (1) and (2). Approval of new sub-type values are to be made through IANA Expert Review.

6. Security Considerations

The IP Traffic Offload Selector 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 IP traffic offload selectors does not introduce any new security vulnerabilities.

7. Acknowledgements

The authors would like to thank Rajesh Pazhyannur, Kent Leung, Mark Grayson, Frank Brockners, Woj Dec, and Steve Wood for all the discussions related to the topic of IP traffic offload. The authors would like to acknowledge the work related SIPTO in 3GPP SA2 working group.

8. References

8.1. 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.

8.2. Informative References

- [RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses", 2010.

Authors' Addresses

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

Email: sgundave@cisco.com

Xingyue Zhou
ZTE Corporation
No.68 Zijinghua Rd
Nanjing
China

Email: zhou.xingyue@zte.com.cn

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

Email: jouni.nospam@gmail.com

Gaetan
Cisco
France

Email: gfeige@cisco.com

Rajeev Koodli
Cisco
3650 Cisco Way
San Jose, CA 95134
USA

Email: rkoodli@cisco.com

NETEXT WG
Internet-Draft
Intended status: Informational
Expires: September 15, 2011

T. Melia, Ed.
Alcatel-Lucent
S. Gundavelli, Ed.
Cisco
March 14, 2011

Logical Interface Support for multi-mode IP Hosts
draft-ietf-netext-logical-interface-support-02.txt

Abstract

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

Status of this Memo

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

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

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

This Internet-Draft will expire on September 15, 2011.

Copyright Notice

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

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

Table of Contents

1. Introduction	4
2. Requirements Language	5
3. Terminology	6
4. Hiding Link-layer Technologies - Approaches and Applicability	7
4.1. Link-layer Abstraction - Approaches	7
4.2. Applicability Statement	8
4.2.1. Link layer support	9
4.2.2. Logical Interface	9
5. Technology Use cases	11
6. Logical Interface Functional Details	12
6.1. Configuration of a Logical Interface	13
6.2. MTU considerations	14
6.3. Supported Link models for a logical interface	14
6.4. Link-layer Identifier of a Logical Interface	15
6.5. ND Considerations for Logical Interface	15
6.6. Logical Interface Forwarding Conceptual Data Structures	16
7. Logical Interface Use-cases in Proxy Mobile IPv6	18
7.1. Multihoming Support	18
7.2. Inter-Technology Handoff Support	19
7.3. Flow Mobility Support	21
8. IANA Considerations	22
9. Security Considerations	23
10. Authors	24
11. Acknowledgements	24

12. References	24
12.1. Normative References	24
12.2. Informative References	25
Authors' Addresses	25

1. Introduction

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

A Logical Interface is a construct internal to the operating system. It is an approach where the link-layer implementations hide the physical interfaces from the IP stack and from the network nodes on the attached access networks. This semantic is widely available in all popular operating systems. Many applications such as Mobile IP client [RFC3775] and IPsec VPN client [RFC4301] rely on this semantic for their protocol implementation and the same semantic can also be useful in this context. Specifically, the mobile node can use the logical interface configuration for leveraging various network-based mobility management features provided by the Proxy Mobile IPv6 domain [RFC5213].

The rest of the document provides the operational details of a Logical Interface on the mobile node and the inter-working between a mobile node using logical interface and network elements in the Proxy Mobile IPv6 domain when supporting some of the mobility management features. It also analyzes the issues involved with this approach and characterizes the contexts in which such usage is appropriate.

2. Requirements Language

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

3. Terminology

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

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

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

VLL-ID (Virtual Link-layer ID) - a virtual link-layer address configured on the logical interface. This identifier can be randomly generated, or configured based on the link-layer address of one of the physical interface.

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

4. Hiding Link-layer Technologies - Approaches and Applicability

There are several techniques/mechanisms that allow hiding access technology changes or movement from host IP layer. This section classifies these existing techniques into a set of generic approaches, according to their most representative characteristics. Later sections of this document analyze the applicability of these solution approaches for supporting features such as, inter-technology handovers and IP flow mobility support for a mobile node in a Proxy Mobile IPv6 domain [RFC5213].

4.1. Link-layer Abstraction - Approaches

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

- o Link-layer Support - Certain link-layer technologies are able to hide physical media changes from the upper layers (see Figure 1). For example, IEEE 802.11 is able to seamlessly change between IEEE 802.11a/b/g physical layers. Also, an 802.11 STA can move between different Access Points (APs) within the same domain without the IP stack being aware of the movement. In this case, the IEEE 802.11 MAC layer takes care of the mobility, making the media change invisible to the upper layers. Another example is IEEE 802.3, that supports changing the rate from 10Mbps to 100Mbps and to 1000Mbps.

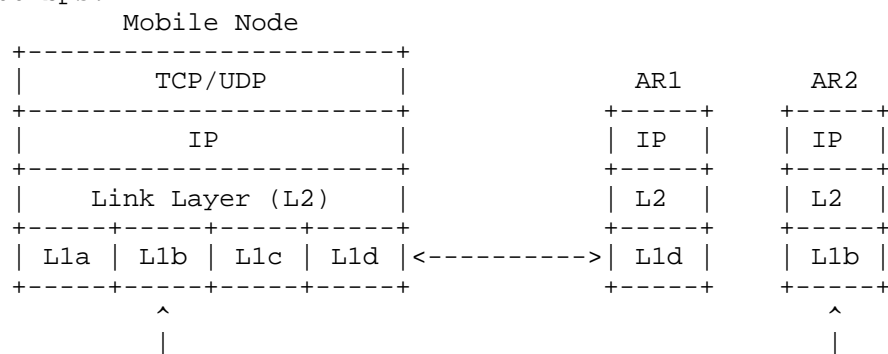


Figure 1: Link layer support solution architecture

There are also other examples with more complicated architectures, like for instance, 3GPP EPC [TS23401]. In this case, a UE can move (inter-RA handover) between GERAN/UTRAN/E-UTRAN, being this movement invisible to the IP layer at the UE, and also to the LMA logical component at the PGW. The link layer stack at the UE (i.e. PDCP and RLC layers), and the GTP between the RAN and the SGW (which plays the role of inter-3GPP AN mobility anchor) hide

this kind of mobility, which is not visible to the IP layer of the UE (see Figure 2).

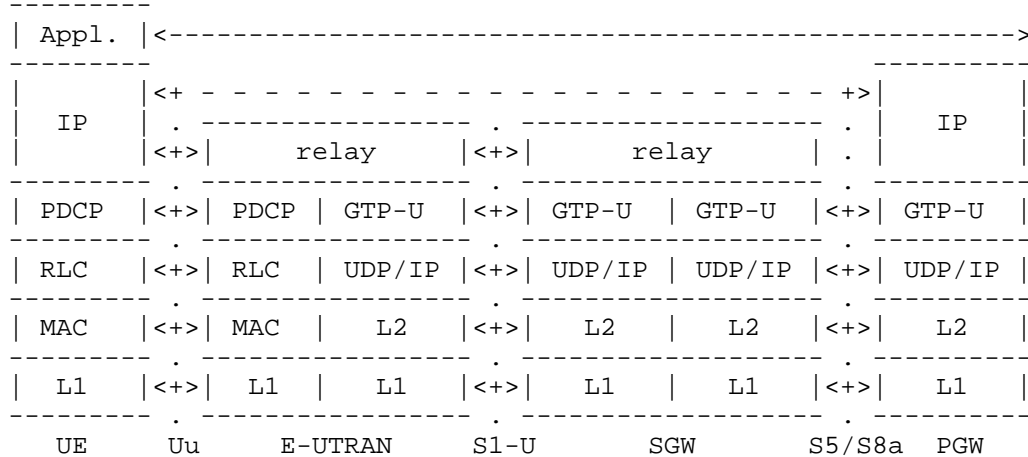


Figure 2: 3GPP LTE/EPC data plane architecture (GTP option)

- o Logical interface: this refers to solutions (see Figure 3) that logically group/bond several physical interfaces so they appear to the upper layers (i.e. IP) as one single interface (where application sockets bind). Depending on the OS support, it might be possible to use more than one physical interface at a time -- so the node is simultaneously attached to different media -- or just to provide a fail-over mode. Controlling the way the different media is used (simultaneous, sequential attachment, etc) is not trivial and requires additional intelligence and/or configuration at the logical interface device driver. An example of this type of solution is the Logical interface, which is defined in this document, or the bonding driver (a Linux implementation).

4.2. Applicability Statement

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

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

4.2.1. Link layer support

Link layer mobility support applies to cases when the same link layer technology is used and mobility can be fully handled at these layers. One example is the case where several 802.11 APs are deployed in the same subnet and all of them share higher layer resources such as DHCP server, IP gateway, etc. In this case the APs can autonomously (or with the help of a central box) communicate and control the STA association changes from one AP to another, without the STA being aware of the movement. This type of scenario is applicable to cases when the different points of attachment (i.e. APs) belong to the same network domain, e.g. Enterprise, hotspots from same operator, etc.

This type of solution does not typically allow for simultaneous attachment to different access networks, and therefore can only be considered for inter-access technology handovers, but not for flow mobility. Existing RFC 5213 handover hint mechanisms could benefit from link layer information (e.g. triggers) to detect and identify MN handovers.

Link layer support is not applicable when two different access technologies are involved (e.g. 802.11 WLAN and 802.16 WiMAX) and the same is true when the same access technology expands over multiple network domains. This solution does not impose any change at the IP layer since changes in the access technology occur at layer two.

4.2.2. Logical Interface

The use of a logical interface allows the mobile node to provide a single interface view to the layers above IP (thus not changing the IP layer itself). Upper layers can bind to this interface, which hides inner inter-access technology handovers or data flow transfers among different physical interfaces.

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

It is therefore clear that the Logical Interface approach satisfies

the multi technology and the sequential vs: simultaneous access support.

5. Technology Use cases

The 3GPP has defined the Evolved Packet Core (EPC) for heterogeneous wireless access. A mobile device equipped with 3GPP and non-3GPP wireless technologies can simultaneously or sequentially connect any of the available devices and receive IP services through any of them. This document focuses on the simultaneous/sequential use of these technologies and on the use cases that derive.

As mentioned in the previous sections the Logical Interface construct is required to hide the specificities of each technology in the context of network based mobility (e.g. in PMIPv6 deployments). The LIF concept can be used with at least the following technologies: 3GPP access technologies (3G, LTE), WIMAX access technology and IEEE 802.11 access technology.

3GPP In most OS implementations the connection setup establishes a PPP interface through the IPCP and IPv6CP protocol [RFC5072]. In this case the PPP interface does not have any L2 address assigned and does not generate any ARP or ND message for layer two address resolution. Conversely recent implementations configure an ethernet alike interface at OS level hiding to the upper layers the PPP nature of the connection. It has been verified (Android platform) that in these cases the ethernet alike interface configures a random L2 MAC address and uses this address as source link layer address in ND messages. ARP is also run between the mobile device and the remote peer (the network is a /30 address space).

WIMAX In WiMAX system also, the connection between the mobile station (MS) and the access router (AR) is a point-to-point link. The MS autoconfigures an address based on the prefix advertised by the AR or is assigned an address via DHCPv6. The stateless address auto-configuration is performed as per [RFC4861] and the IPv6 address is formed by adding an IID to the prefix learnt from Router Advertisement. IPv6 packets sent or received by the MS are identified by specific IDs, by which the AR can map them to the corresponding tunnel in the network.

WIFI TBD

IPsec TBD

6. Logical Interface Functional Details

On most operating systems, a network interface is associated with a physical device that offers the services for transmitting and receiving IP packets to the applications on the host. In some configurations, a network interface can also be implemented as a logical interface which does not have the inherent capability to transmit, or receive packets on a physical medium, but relies on other physical interfaces for such services. Example of such configuration is an IP tunnel interface. General overview of a logical interface is shown in Figure 3. This section identifies the functional details of a logical interface and provides some implementation considerations.

The logical interface allows heterogeneous attachment while leaving the change in the media transparent to the IP stack. Simultaneous and sequential network attachment procedures are possible enabling inter-technology and flow mobility scenarios.

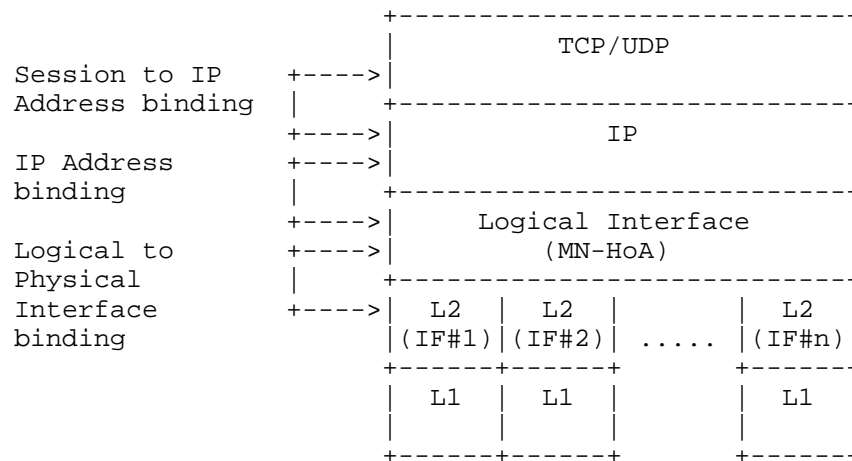


Figure 3: General overview of logical interface

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

- o P1: The logical interface has a relation to a set of physical interfaces (sub-interfaces) on the host that it is abstracting. These sub-interfaces can be attached or detached from the Logical Interface at any time. The sub-interfaces attached to a Logical interface are not visible to the IP and upper layers.
- o P2: The logical Interface may either use a virtual interface identifier independent of the interface identifiers of its sub-interfaces, or it may use the link-layer identifier from one of its sub-interfaces.
- o P3: Logical Interface has the path awareness with respect to the attached IP networks. For example, the logical interface may be bound to two IP networks, CAFE::/64 and BABA::/64, each of these prefixes may have been hosted on access networks attached through different sub-interfaces, WLAN and LTE. The logical interface has the path awareness with respect to IP network to sub-interface mapping.
- o P4: Logical Interface may be attached to multiple access technologies with different link MTU values. The adopted MTU value for the logical interface must be lowest MTU value across those access technologies.
- o P5: The Send/Receive functions of the Logical interface are mapped to the services exposed by the sub-interfaces. This mapping is dynamic and any change is not visible to the upper layers of the IP stack.
- o P6: Logical interface adapts to the link model underneath where the packet is being transmitted. When transmitting a packet on a sub-interface which is attached to a p2p link, the transmission conforms to the p2p link model and when transmitting on a sub-interface attached to a shared link, the transmission conforms to the shared link model.
- o P7: The Logical interface maintains IP flow information for each of its sub-interfaces. A conceptual data structure can be maintained for this purpose. The host may populate this information based on tracking each of the sub-interface for the active flows.

6.1. Configuration of a Logical Interface

A host may be statically configured with the logical interface configuration, or an application such as a connection manager on the host may dynamically create it. Furthermore, the set of sub-interfaces that are part of a logical interface construct may be a

fixed set, or may be kept dynamic, with the sub-interfaces getting added or deleted as needed. The specifics on how a host creates a logical interface, or how it decides to add or delete a sub-interface to a logical interface is outside the scope of this document.

6.2. MTU considerations

The link MTU (maximum transmission unit) value configured on a logical interface should be the lowest of the MTU values supported across any of the physical interfaces that are part of that logical interface construct. The MTU value should be configured as part of the logical interface creation on the host.

Furthermore, this value must be updated any time there is a change to the logical interface construct, such as when interfaces are added or deleted from the logical interface setup. Any time there is an inter-technology handover between two access technologies, the applications on the host bound to the IP address configuration on the logical interface will not detect the change and will continue to use the MTU value of the logical interface for the outbound packets, which is never greater than the MTU value on that supported access network. However, the access network may continue to deliver the packets conforming to the MTU value supported on that access technology and the logical interface should be able to receive those packets from the physical interface attached to that network.

6.3. Supported Link models for a logical interface

The sub-interfaces of a logical interface can be bound to a point-to-point or a shared link (Example: LTE and WLAN). The logical interface appears as a shared-link to the applications, and adapts to the link model of the sub-interface for packet communication. For example, when transmitting a packet on a sub-interface which is attached to a p2p link, the transmission conforms to the p2p link model and when transmitting on a sub-interface attached to a shared link, the transmission conforms to the shared link model.

Based on the link to which the sub-interface is attached to, the layer-2 resolutions may or may not be needed. If the interface is bound to a P2P link with PPP running, there will not be any link-layer resolutions in the form of ARP/ND messages. However, if the interface is bound to a shared link such as Ethernet, there will be ND resolutions. The logical interface implementation has to maintain the required link model and the associated state for each sub-interface.

6.4. Link-layer Identifier of a Logical Interface

The logical Interface may or may not use the link-layer identifier from one of its sub-interfaces. Following are the considerations.

- o In access architectures where it is possible to adopt a virtual link-layer identifier and use it for layer-2 communications in any of the access networks, a virtual identifier (VLL-Id) may be used. The specifics on how that identifier is chosen is out side the scope of this document. This identifier may be used for all link-layer communications. This identifier may also be used for generating IPv6 global or link-local addresses on that interface.
- o In access architectures, where the link-layer identifier is associated with a specific access technology, it will not be possible for the logical interface to adopt a virtual identifier and it use it across different access networks. In such networks, the logical interface must adopt the identifier of the respective sub-interface through which a packet is being transmitted.

6.5. ND Considerations for Logical Interface

The following are the Neighbor Discovery related considerations for the logical interface.

- o Any Neighbor Discovery messages, such as Router Solicitation, Neighbor Solicitation messages that the host sends to a multicast destination address of link-local scope such as, all-nodes, all-routers, solicited-node multicast group addresses, using either an unspecified (::) source address, or a link-local address configured on the logical interface will be replicated and forwarded on each of the sub-interfaces under that logical interface. However, if the destination address is a unicast address and if that target is known to exist on a specific sub-interface, the message will be forwarded only on that specific sub-interface.
- o Any Neighbor Discovery messages, such as Router Advertisement, that the host receives from any of its sub-interfaces, will be associated with the logical interface, i.e., in some implementations the message will appear on the input interface of the logical interface.
- o When using Stateless Address Autoconfiguraion [RFC4862] for generating IPv6 address configuration on the logical interface, the host may use any of the IPv6 prefixes received from the Router Advertisement messages that it received from any of its sub-interfaces.

- o The response to a Neighbor Discovery message received for a unicast, link-specific multicast group address, will be sent on the same sub-interface path where the packet was received.
- o When using DHCPv4 for obtaining address configuration for the logical interface, the value in the chaddr field in the DHCP messages will be based on the link-layer identifier scheme chosen by the logical interface.

.

6.6. Logical Interface Forwarding Conceptual Data Structures

The LIF should maintain the LIF and FLOW table data structures depicted in Figure 4

LIF TABLE		FLOW table	
+=====+		+=====+	
PIF_ID	FLOW RoutingPolicies	FLOW ID	PIF_ID
	Home Network Prefix	+-----+	
	Link Layer Address	FLOW_ID	PIF_ID
	Status	+=====+	
+-----+			
PIF_ID	FLOW RoutingPolicies		
	Home Network Prefix		
	Link Layer Address		
	Status		
+-----+			
....		
+=====+			

Figure 4

The LIF table maintains the mapping between the LIF and each PIF associated to the LIF (see P3). For each PIF entry the table should store the associated Routing Policies, the Home Network Prefix received during the SLAAC procedure, the configured Link Layer Address (as described above) and the Status of the PIF (e.g. active, not active).

The method by which the Routing Policies are configured in the UE is out of scope of this document. It is however assumed that this method is in place and that these policies are configured in the LIF TABLE.

The FLOW table allows a LIF to properly route each IP flow to the right interface (see P6). The LIF can identify flows arriving on its

PIFs and can map them accordingly for transmitting the corresponding packets. For locally generated traffic (e.g. unidirectional outgoing flows, mobile initiated traffic, etc.), the LIF should perform interface selection based on the Flow Routing Policies. In case traffic of an existing flow is suddenly received from the network on a different PIF than the one locally stored, the LIF should interpret the event as an explicit flow mobility trigger from the network and it should update the PIF_ID parameter in the FLOW table. Similarly, locally generated events from the PIFs or configuration updates to the local policy rules can cause updates to the table and hence trigger flow mobility.

7. Logical Interface Use-cases in Proxy Mobile IPv6

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

7.1. Multihoming Support

A mobile node with multiple interfaces can attach simultaneously to the Proxy Mobile IPv6 domain. Each of the attachment links are assigned a unique set of IPv6 prefixes. If the host is configured to use Logical interface over the physical interface through which it is attached, following are the related considerations.

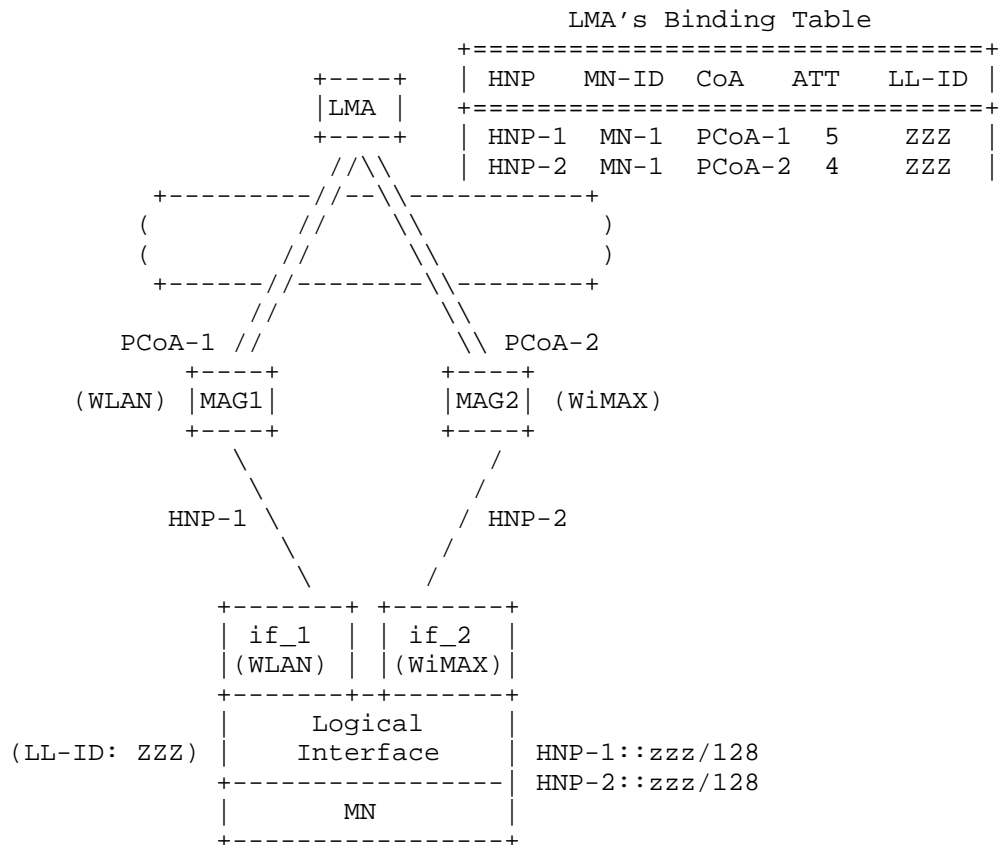


Figure 5: Multihoming Support

- o The mobile node detects the advertised prefixes from the MAG1 and MAG2 as the on link prefixes on the link to which the Logical interface is attached.
- o The mobile node can generate address configuration using stateless auto configuration mode from any of those prefixes.
- o The applications can be bound to any of the addresses bound to the Logical interface and that is determined based on the source address selection rules.
- o The host has path awareness for the hosted prefixes based on the received Router Advertisement messages. Any packets with source address generated using HNP_1 will be routed through the interface if_1 and for packets using source address from HNP_2 will be routed through the interface if_2.

7.2. Inter-Technology Handoff Support

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

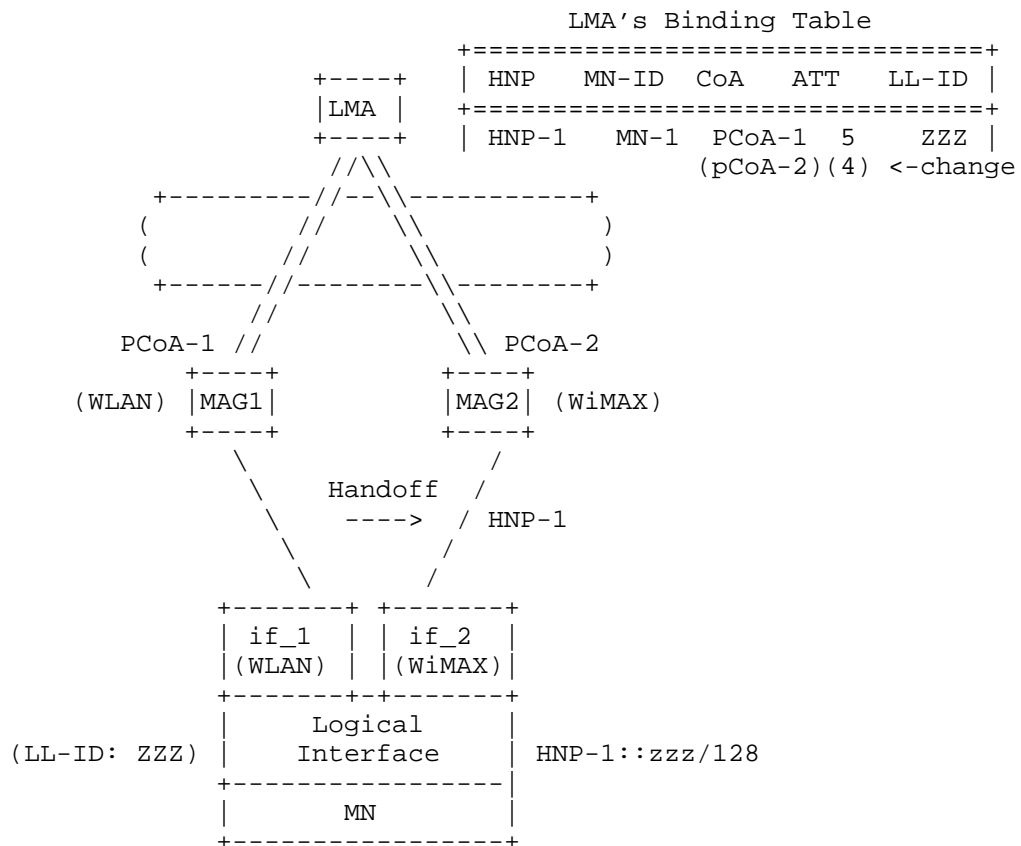


Figure 6: Inter-Technology Handoff Support

- o When the mobile node performs an handoff between if_1 and if_2, the change will not be visible to the applications of the mobile node. It will continue to receive Router Advertisements from the network, but from a different sub-interface path.
- o The protocol signaling between the network elements will ensure the local mobility anchor will switch the forwarding for the advertised prefix set from MAG1 to MAG2.
- o The MAG2 will host the prefix on the attached link and will include the home network prefixes in the Router Advertisements that it sends on the link.

7.3. Flow Mobility Support

For supporting flow mobility support, there is a need to support vertical handoff scenarios such as transferring a subset of prefix(es) (hence the flows associated to it/them) from one interface to another. The mobile node can support this scenario by using the Logical interface support. This scenario is similar to the Inter-technology handoff scenario defined in Section 7.2, only a subset of the prefixes are moved between interfaces.

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

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

8. IANA Considerations

This specification does not require any IANA Actions.

9. Security Considerations

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

10. Authors

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

Carlos Jesus Bernardos Cano

cjbc@it.uc3m.es

Antonio De la Oliva

aoliva@it.uc3m.es

Yong-Geun Hong

yonggeun.hong@gmail.com

Kent Leung

kleung@cisco.com

Tran Minh Trung

trungtm2909@gmail.com

Hidetoshi Yokota

yokota@kddilabs.jp

Juan Carlos Zuniga

JuanCarlos.Zuniga@InterDigital.com

11. Acknowledgements

The authors would like to acknowledge prior discussions on this topic in NETLMM and NETEXT working groups. The authors would also like to thank Joo-Sang Youn, Pierrick Seite, Rajeev Koodli, Basavaraj Patil, Julien Laganier for all the discussions on this topic.

12. References

12.1. Normative References

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

- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", September 2007.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

12.2. Informative References

- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
- [RFC5072] Varada, S., "IP Version 6 over PPP", September 2007.
- [RFC5677] Melia, T., Bajko, G., Das, S., Golmie, N., and JC. Zuniga, "IEEE 802.21 Mobility Services Framework Design (MSFD)", RFC 5677, December 2009.
- [RFC6085] Gundavelli, S., Townsley, M., Troan, O., and W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", RFC 6085, January 2011.
- [TS23401] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.", 2009.

Authors' Addresses

Telemaco Melia (editor)
Alcatel-Lucent
Route de Villejust
Nozay 91620
France

Email: telemaco.melia@alcatel-lucent.com

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

Email: sgundave@cisco.com

NETEXT WG
Internet-Draft
Intended status: Informational
Expires: October 24, 2011

S. Gundavelli
Cisco
M. Liebsch
NEC
April 22, 2011

PMIPv6 inter-working with WiFi access authentication
draft-liebsch-netext-pmip6-authiwb-02.txt

Abstract

Proxy Mobile IPv6, the IETF's protocol for network-based mobility management, requires a completed and successful authentication of the mobile node before it is registered at the mobility anchor. This document describes inter-working between access authentication mechanisms, such as IEEE 802.1X, and the Proxy Mobile IPv6 protocol to enable trusted WiFi access to a network-based mobility management domain. Furthermore, the use of authentication method specific identifiers for unique identification of mobile nodes during setup and maintenance of their mobility session is described, following recommendations of related standards organizations, such as 3GPP and the WiMAX Forum.

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 October 24, 2011.

Copyright Notice

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

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

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

Table of Contents

1. Introduction	3
2. Conventions and Terminology	5
3. Functional Objectives	6
4. Inter-working with IEEE 802.1X EAP	9
4.1. General use with authentication against a RADIUS Server	9
5. Security Considerations	11
6. IANA Considerations	12
7. Normative References	13
Authors' Addresses	14

1. Introduction

Proxy Mobile IPv6 (PMIPv6) [RFC5213] represents the IETF's protocol for network-based mobility management and is being deployed in various standards, such as the 3rd Generation Partnership Project (3GPP), to complement host mobility. According to the PMIPv6 standard, mobile nodes (MN) do not require a secure interface to the mobility anchor (LMA), as there is no direct signaling for mobility management between the MN and the LMA, but the Mobility Access Gateway (MAG) sets up and maintains a mobility binding on the LMA on behalf of the host by means of a Proxy Binding Update (PBU). [RFC5213] requires a successful authentication of the MN before the MAG sends a PBU to the LMA to set up a mobility binding for the MN. Furthermore, it assumes the MAG to be informed about a mobile node identifier (MN-Identifier), which unambiguously identifies the MN during the mobility session. Such MN-Identifier can be a static identifier or a temporary identifier, which may be derived from a static identifier.

This document intends to provide guidelines for PMIPv6 to inter-work with access authentication protocols which have been designed for IEEE 802-type of link technologies. Initial versions of this document focus on IEEE 802.1X and its recommendation to use the Extensible Authentication Protocol (EAP) [RFC3748]. Based on the procedure for general inter-working, more specific use cases are documented for discussion and reference. These use cases include the use of the Wireless LAN technology according to the IEEE 802.11 standard to provide trusted access to 3GPP's packet core network. So far, WLAN has been considered as untrusted access being even provided by third parties and MNs connect through WLAN to the mobile operator network through an established secure tunnel. Stepping towards WLAN trusted access avoids the overhead of an established IPsec tunnel with a packet data gateway in the operator's core network, but requires inter-working between WLAN access authentication and the operator's authentication and identification mechanisms. In the context of trusted WLAN access and network-based mobility management, WLAN security is being used to protect traffic on the wireless link whereas the trust relationship between a MAG and the LMA is used to convey traffic through the operator's core network.

The first version of this document discusses inter-working between IEEE 802.1X EAP and PMIPv6 as well as some specific use cases for trusted WLAN access in 3GPP's evolved packet core, which are based on recommended authentication schemes, such as EAP-AKA [RFC5448]. Further use cases with different EAP authentication schemes as well as inter-working between PMIPv6 and web authentication will be added to future versions of this document. Prior to describing details of PMIPv6 inter-working with various access authentication schemes in

Section 4, Section 3 describes functional objectives to enable trusted WLAN access to mobile operator networks and efficient inter-working between WiFi access authentication and operators' mobility management as well as policy and AAA infrastructure.

2. Conventions and Terminology

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

This document uses the terminology of [RFC5213]. The following additional terms are used in the context of this draft:

- o AAA -- Authentication, Authorization and Accounting
- o EAP -- Extensible Authentication Protocol
- o PCC -- Policy and Charging Control
- o PMK -- Pairwise Master Key

3. Functional Objectives

Major motivation and objective to document inter-working between WiFi access authentication and PMIPv6 is to describe complete system operation, message sequences and identification schemes for network-based mobility management using PMIPv6 including IEEE 802.11-based access as proven and widely accepted radio technology and associated authentication mechanisms. Inter-action between access authentication and mobility management allows the specification of missing components in [RFC5213], mainly referring to MAG operation being triggered by successful MN authentication and MN identification.

The relevance of WiFi radio access is proven by various standards' initiative in specifying inter-working with IEEE 802.11-based technology. One example is the 3GPP's interest in supporting traffic offload to WLAN networks. Another example is the WiMax Forum's Network Architecture, which consider a WiFi-WiMAX inter-working function to enable access to the WiMAX network through WiFi radio access and to support handover between WiFi and WiMAX radio access.

The PMIPv6 standard [RFC5213] assumes a completed and successful access authentication of MNs (or their subscriber) before the MAG registers the MN at an LMA by means of a PBU. One objective of this document is to analyze relevant access authentication schemes and to document the operation of PMIPv6 in dependency of these authentication mechanisms. The EAP procedure as IEEE 802.X recommendation is being considered most relevant at this time. Web-authentication is a further popular access authentication scheme, which can be analyzed and inter-working with PMIPv6 can be specified, even though manual subscriber inter-action during access authentication conflicts with automatic and seamless operation, e.g. during dual radio handover from 3GPP access to WiFi access.

A further objective is to analyze the details of preferred authentication schemes, taking 3GPP and WiMAX Forum recommendations into account, and to document the use of common identifiers for access authentication and PMIPv6-based mobility management. Such identifier-specific inter-working must take further requirements, such as unique identification of a MN during the mobility session, into account. Some identifiers, which are generated during access authentication, are unique for an MN, but are not stable and valid beyond a certain radio access point. In such case, the MAG must use a different identifier or resolve such temporary identifier into a unique identifier which is valid beyond a single access point and MAG.

A further goal is to analyze inter-working between access

authentication schemes and PMIPv6 during handover, which may also imply a change in the radio access technology. Treatment of authentication methods, keys and identifiers and associated inter-working with PMIPv6 operation is documented.

Figure 1 depicts a high-level view of a WiFi network being integrated into a mobile operator network as trusted access. Instead of using a Security and Mobility Gateway, such as the 3GPP's Packet Data Gateway (PDG), which terminates an IPsec tunnel with the UE, the system relies on concatenated protected links between the UE and the WiFi access network, as well as between the WiFi access network and the LMA. The illustrated setup assumes a MAG function to be co-located with the WiFi Access Point or a WiFi Controller (Ctrlr). Inter-working between WiFi access authentication, PMIPv6 operation and the operator network's AAA and PCC (Policy and Charging Control) infrastructure is achieved by means of associated interfaces with the LMA. Future extensions may consider a direct policy configuration interface with the WiFi access network controller. This version of the inter-working document does not assume a direct policy control interface between the WiFi access network and the operator's PCC system. If needed, the PMIPv6 protocol interface may be proposed to convey associated information. Policy configuration in the WiFi access network is considered out of scope of this documentation.

4. Inter-working with IEEE 802.1X EAP

4.1. General use with authentication against a RADIUS Server

IEEE 802.1X recommends EAP for access authentication, which can make use of an Authentication Server using for example the RADIUS protocol between the Authenticator and the Authentication Server. [RFC3579] specifies RADIUS extensions to convey EAP attributes between an Authenticator and the RADIUS server. Figure 2 depicts general inter-working between PMIPv6 and IEEE 802.1X using EAP.

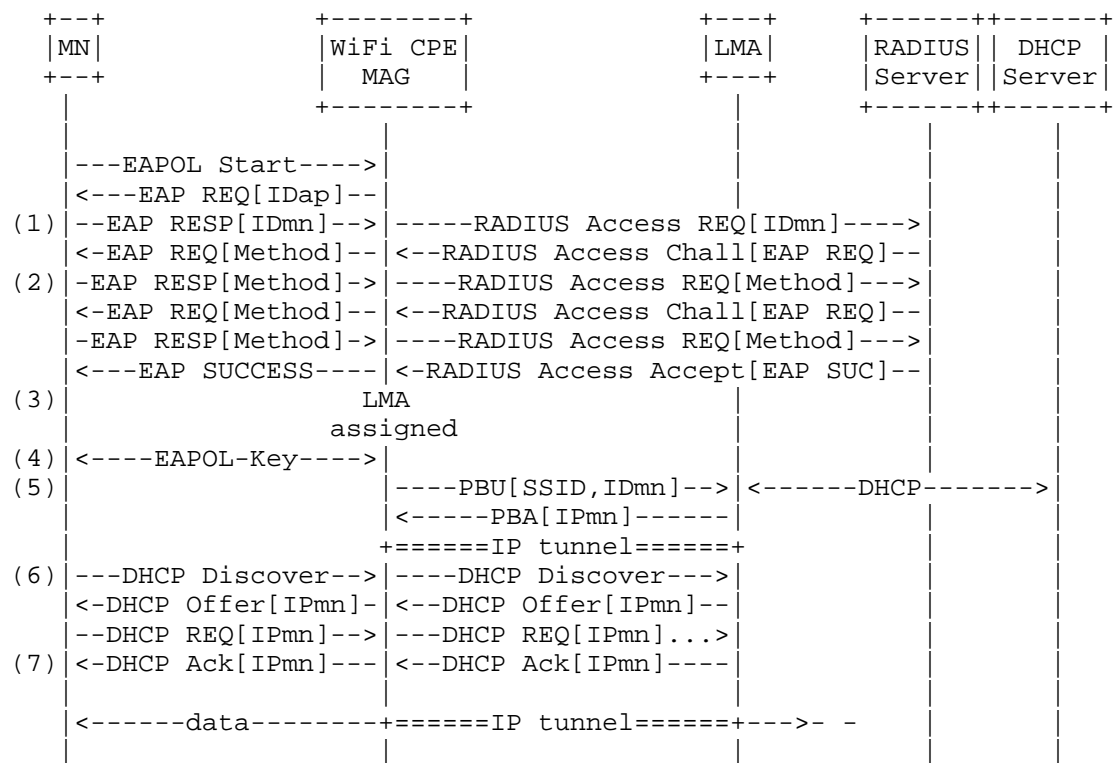


Figure 2: PMIPv6 inter-working with WPA2-802.1X access authentication against a RADIUS server

After the MN has associated with a WiFi Access Point, the EAPOL procedure starts (1). EAP attributes are mapped by the WiFi AP/Ctrlr

between EAPOL on the wireless link and RADIUS operation on the link towards the RADIUS server. The RADIUS server selects one or multiple authentication methods, which are performed with the MN in a challenge-response procedure (2). As a result of a successful EAP procedure, the RADIUS server may assign an LMA to the MN and signal the LMA identifier or the LMA IP address to the MAG function in the WiFi access network (3). The MN and the WiFi Access Point can now negotiate the Session Key to protect the wireless access (4). At that time, the MAG can take the EAP success as trigger to initiate the PBU registration of the MN with the LMA (5). The keys and identifiers being used and generated differ between the EAP and authentication method. In general, the MAG should not use the generated Session Key or security association identifier, as scope is limited to the the MN's association with the Access Point. More suitable is an identifier being negotiated during the authentication procedure with the RADIUS server, e.g. based on the Pairwise Master Key (PMK) or any identifier which derives from the PMK without including single Access Point specific information, such as the AP's MAC address. One example, which will be described in more detail in future versions of this document, is the use of the International Mobile Subscriber Identity (IMSI) to derive a NAI at the Authentication Server. This IMSI-based NAI is then used as MN-Identifier in the PBU. Such approach is being proposed in 3GPP for trusted access to the mobile operator network through non-3GPP type radio access networks [3GPP-TS23.402] [3GPP-TS33.402].

As a result of the MN's registration, the LMA performs DHCP with a DHCP server to retrieve a valid IP address for the MN (IP_{MN}). The assigned IP address is then signaled to the MAG in the PBA. The MN learns about this IP address from the DHCP procedure (6). After successful completion of the DHCP procedure (7), the MN can use the protected wireless link to communicate with the network infrastructure.

5. Security Considerations

This document analyzes and documents inter-working between WiFi access authentication and PMIPv6 mobility management to enable trusted access to a mobile operator network which uses network-based mobility management. The document refers to standard operation of PMIPv6 [RFC5213] as well as well accepted WiFi authentication mechanisms, such as EAP using a RADIUS server as authentication server, without introducing new messages or message sequences. Solely the inter-working of access authentication and PMIPv6 is described by means of message sequence charts. Furthermore, the use of identifiers, which are built during access authentication, for MN identification in the PMIPv6-based mobility management protocol is described. Hence, the documented inter-working should not introduce any new security threats.

6. IANA Considerations

This document is based on standardized protocols for WiFi access authentication and network-based mobility management. No additional protocol messages and options are specified so far in this document.

7. Normative References

[3GPP-TS23.402]

"3GPP TS 23.402; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 10)", <<http://www.3gpp.org>>.

[3GPP-TS33.402]

"3GPP TS 33.402; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 9)", <<http://www.3gpp.org>>.

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

[RFC3579] Aboba, B. and P. Calhoun, "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", RFC 3579, September 2003.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

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

Authors' Addresses

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

Email: sgundave@cisco.com

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

Email: liebsch@neclab.eu

netext
Internet-Draft
Intended status: Standards Track
Expires: January 12, 2012

X. Zhou
ZTE Corporation
J. Korhonen
Nokia Siemens Networks
C. Williams
Consultant
July 11, 2011

Prefix Delegation for Proxy Mobile IPv6
draft-zhou-netext-pd-pmip-01.txt

Abstract

This document explains how network mobility and DHCPv6-based Prefix Delegation works with Proxy Mobile IPv6.

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 12, 2012.

Copyright Notice

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

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

Table of Contents

1. Introduction	3
2. Convention & Terminology	4
3. DHCPv6 Prefix Delegation for PMIPv6	5
3.1. Assumption	5
3.2. Network Mobility Service	5
3.3. Binding association with the delegated prefix	6
3.3.1. Mobile Router initiated prefix delegation in PMIPv6	6
3.3.2. Mobile Router refresh prefix delegation in PMIPv6	7
3.4. Mobile Access Gateway Operation	7
3.4.1. Extension to Binding Update List Entry Data Structure	7
3.4.2. Forwarding	8
3.4.3. Handover	8
3.5. Local Mobility Anchor Operation	9
3.5.1. Extension to Binding Cache Entry Data Structure	9
3.5.2. Forwarding	9
4. Security Considerations	10
5. IANA Considerations	11
6. Normative References	12
Authors' Addresses	13

1. Introduction

DHCPv6 prefix delegation [RFC 3633] (DHCPv6PD) can be used to assign mobile network prefix(es) to a Mobile Router as specified in DHCPv6 Prefix Delegation for NEMO [draft-ietf-mext-nemo-pd-07]. However, there is a gap currently for this NEMO support in PMIPv6 architecture. If a mobile router (MR) is provided Proxy Mobile IPv6 Protocol as its mobility management when connecting the network and use DHCPv6PD to obtain prefix(es) for the nodes in the mobile network behind the MR, currently neither the Mobile Access Gateway (MAG) nor the Local Mobility Anchor (LMA) can be able to identify the packet including delegated prefix(es). When the MR (Requesting Router) uses DHCPv6 PD to obtain the delegated prefix(es), these prefix(es) SHOULD be associated with the PMIPv6 binding. Otherwise the packets addressed to the delegated prefix will be discarded by the MAG or the LMA. This document describes extension to PMIPv6 for supporting prefix delegation.

2. Convention & 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].

All the mobility related terms used in this document are to be interpreted as defined in Mobile IPv6 [RFC 3775], Network Mobility Basic Support protocol [RFC 3963], Proxy Mobile IPv6 specification [RFC 5213], DHCPv6 Prefix Delegation for NEMO [draft-ietf-mext-nemo-pd-07], DHCP Prefix Delegation [RFC3633] and Mobility Related Terminology [RFC 3753]. This document does not define any new terms.

3. DHCPv6 Prefix Delegation for PMIPv6

3.1. Assumption

This specification extends PMIPv6 to assign not only the home network prefix but also the mobile network prefix for supporting network mobility. It assumes that a MR is a regular IPv6 router without extension for mobility managements. The MR sends the packets from its mobile network to the MAG and the MAG delivers the packets to the mobile network via the MR.

In order to use DHCPv6PD as mobile network prefix assignment mechanism in mobile networks, this specification has following assumptions.

- o The Mobile Router MUST play the role of the Requesting Router.
- o The Delegating Router can be located either at LMA or some other device in the PMIPv6 domain.
- o The MAG MUST play the role of DHCPv6 Relay Agent to intercept the related DHCPv6 message from the Mobile Router.
- o The Mobile Router (Requesting Router) MUST obtain the home network prefix before initiating the DHCPv6 prefix delegation procedure.
- o All the mobile network prefixes managed in the Delegating Router MUST be reachable via local mobility anchor.
- o The Mobile Router (Requesting Router) SHOULD support Prefix Exclude Option for DHCPv6-based Prefix Delegation as described in [draft-ietf-dhc-pd-exclude].

3.2. Network Mobility Service

The network mobility service of a mobile router is managed by the mobile node's policy profile defined in [RFC 5213]. During mobile router initial attachment procedure, the mobile access gateway MUST identify the mobile router and acquire the mobile router!_s policy profile to determine whether the network mobility service is offered to the mobile router. If the network mobility service needs to be offered to the mobile node, the mobile access gateway MUST set the Mobile Router Flag (R) when sending the Proxy Binding Update message to the local mobility anchor.

3.3. Binding association with the delegated prefix

3.3.1. Mobile Router initiated prefix delegation in PMIPv6

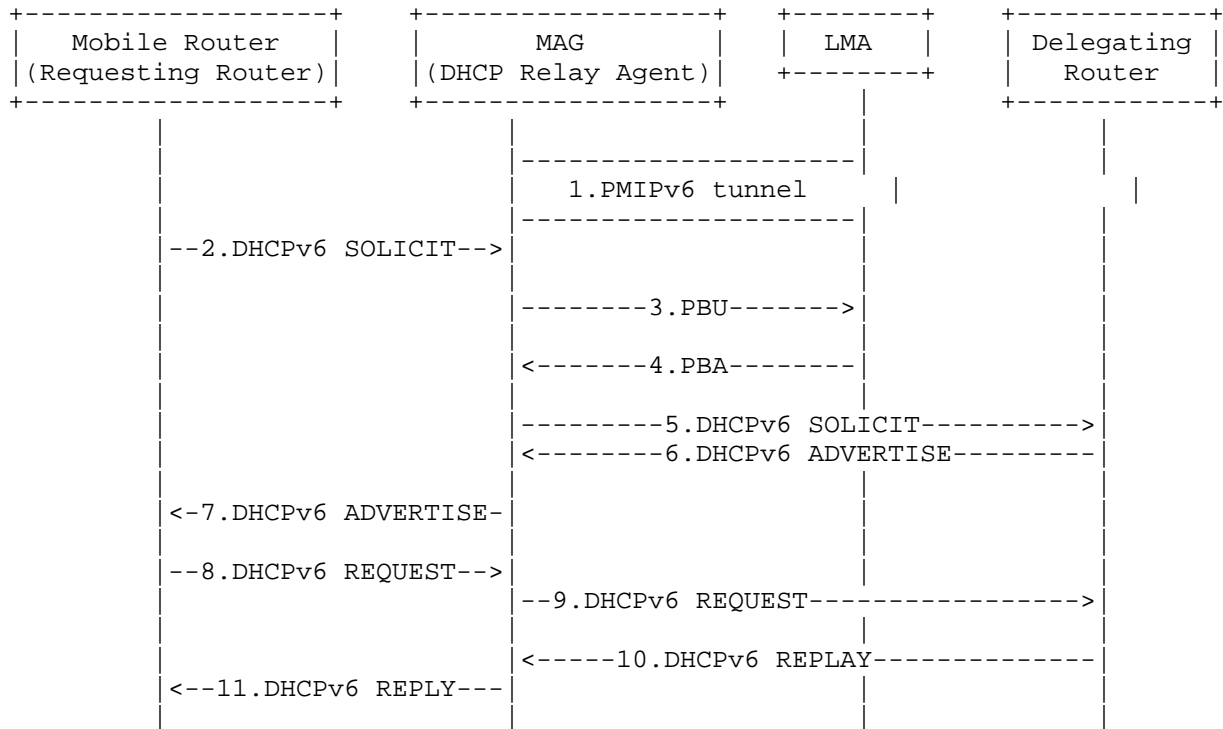


Figure 1: Prefix Delegation in PMIPv6

The steps of the procedure in Figure 1 are as following.

1. The PMIPv6 tunnel is set up between the MAG and LMA. The MAG plays function of DHCPv6 relay agent between the MN and the DHCPv6 server and intercept all the DHCP related messages.

2. The mobile router which acts as a "Requesting Router" as described in [RFC 3633] sends DHCPv6 SOLICIT message including one or more IA_PD option(s) to the MAG to acquire the delegated prefix(es).

3. Upon receiving DHCPv6 SOLICIT the MAG sends a Proxy Binding Update message including a Mobile Network Prefix mobility option as defined in Section 4.3 of [RFC 3963] to the LMA. All the considerations from Section 5.3.1 of [RFC 5213] MUST be applied on the encapsulated Proxy Binding Update message.

4. On reception of the Proxy Binding Update the LMA returns the assigned prefix in the Mobile Network Prefix option carried by a Proxy Binding Acknowledgment to the MAG. The assigned prefix is the same one which will be assigned via DHCPv6PD in step 6 which MUST be added the delegated prefix(es) in its binding cache which is extended as in Section 3.5.1.

5. The DHCPv6 relay agent on the MAG as described in [RFC 3315] relays the DHCPv6 SOLICIT message to the delegation router. NOTE: Step 3 and Step 5 are processed in parallel.

6. The delegating router inserts one or more IA_PD option(s) including the delegated prefix(es) and send it to the MAG (DHCPv6 relay agent) via the DHCPv6 ADVERTISE message.

7. The MAG relays the DHCPv6 ADVERTISE message to the MN.

8. The MN sends DHCPv6 REQUEST message with the IA_PD option(s) received from previous message to the MAG (DHCPv6 relay agent).

9. The MAG relays the DHCPv6 REQUEST message to the delegating router.

10. The delegating router responses the REQUEST to the MAG via DHCPv6 REPLY message.

11. The MN receives one or more IA_PD prefix(es) in the DHCPv6 REPLY message from the MAG.

3.3.2. Mobile Router refresh prefix delegation in PMIPv6

When the mobile router sends DHCPv6 Renew messages to extend the lifetime of the delegated prefix, the messages are also intercepted by the MAG and relayed to the delegating router. If the MAG finds that the lifetime of the delegated prefix which is stored in the IA_PD Prefix Option carried by the DHCPv6 reply message set to zero, the MAG SHOULD triggers a Proxy Binding Update to remove the binding for that mobile network prefix.

3.4. Mobile Access Gateway Operation

3.4.1. Extension to Binding Update List Entry Data Structure

In order to support this specification, the conceptual Binding Cache entry data structure needs to be extended with a new prefix information field as [RFC 3963] does. This prefix information field is used to store the mobile network prefix information which is assigned to the mobile router in the Proxy Binding Acknowledgement

during the procedure of Binding association with the delegated prefix in section 3.2.

3.4.2. Forwarding

Forwarding packets sent to the mobile router!_s mobile network prefix

- o On receiving a packet from the bi-directional tunnel established with the mobile router!_s local mobility anchor, the mobile access gateway MUST use the destination address of the inner packet to forward it on the interface where the destination mobile network prefix is hosted.

Forwarding packets sent by the mobile router

- o On receiving a packet from a mobile router connected to its access link, the mobile access gateway MUST ensure that there is an established binding for that mobile router with its local mobility anchor before tunneling the packet to the mobile router!_s local mobility anchor.

All other considerations from 6.10.5 MUST be applied here also.

3.4.3. Handover

When the mobile router moves from the previously attached mobile access gateway to the newly attached mobile access gateway, the newly attached mobile access gateway MAY know the mobile network prefix which is assigned during the previous attachment from some network element, e.g. from the previous mobile access gateway. It is out of scope of this specification that how the newly attached mobile access gateway obtains the previously assigned mobile network prefix. After handover to the new mobile access gateway, a Proxy Binding Update message including the assigned mobile network prefix (if available) MUST be sent from the new mobile access gateway to the local mobility anchor. The local mobility anchor MUST check the mobile network prefix in the Proxy Binding Update message and return the same assigned mobile network prefix in the Proxy Binding Acknowledgement message. If the previously assigned mobile network prefix is not available in the new mobile access gateway, the new mobile access gateway MUST contain the mobile network prefix set with 0 in the Proxy Binding Update message. In this case, the local mobility anchor MUST return the same previously assigned mobile network prefix in Proxy Binding Acknowledgement.

3.5. Local Mobility Anchor Operation

3.5.1. Extension to Binding Cache Entry Data Structure

In order to support this specification, the conceptual Binding Cache entry data structure needs to be extended with a new prefix information field as [RFC 3963] does. This prefix information field is used to store the mobile network prefix information which is assigned to the mobile router in the Proxy Binding Acknowledgement during the procedure of Binding association with the delegated prefix in section 3.2.

3.5.2. Forwarding

Intercepting packets sent to the mobile router!_s mobile network prefix

- o When the local mobility anchor is serving to the mobile router, it MUST be able to receive packets those are sent to the mobile router!_s mobile network. In order to receive those packets, the mobile access gateway MUST advertise a connected route into the Routing Infrastructure for the mobile router!_s mobile network prefix(es).

Forwarding packets to the mobile router

- o On receiving a packet from a correspondent node with the destination address matching the mobile router!_s mobile network prefix(es) the local mobility anchor MUST forward the packet through the bi-directional tunnel set up for that mobile router.

All other considerations from 5.6.2 MUST be applied here also.

4. Security Considerations

All security considerations from the base Proxy Mobile IPv6 [RFC 5213], DHCPv6 Prefix Delegation specification [RFC 3633] apply when using the extensions defined in this document.

5. IANA Considerations

This document reuses the mobile network prefix option defined in [RFC 3963] in Proxy Mobile IPv6 to assign the mobile network prefix via DHCPv6 for prefix delegation. It does not introduce any additional IANA considerations.

6. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

Authors' Addresses

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

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

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

Email: jouni.nospam@gmail.com

Carl Williams
Consultant
San Jose, CA
USA

Email: carlw@mcsr-labs.org

