Internet Engineering Task Force (IETF)
Request for Comments: 6097
Category: Informational
ISSN: 2070-1721

J. Korhonen
Nokia Siemens Networks
V. Devarapalli
Vasona Networks

February 2011

Local Mobility Anchor (LMA) Discovery for Proxy Mobile IPv6

Abstract

Large Proxy Mobile IPv6 deployments would benefit from a functionality where a Mobile Access Gateway could dynamically discover a Local Mobility Anchor for a Mobile Node attaching to a Proxy Mobile IPv6 domain. The purpose of the dynamic discovery functionality is to reduce the amount of static configuration in the Mobile Access Gateway. This document describes several possible dynamic Local Mobility Anchor discovery solutions.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6097.

Table of Contents

1. Introduction

A Proxy Mobile IPv6 (PMIPv6) [RFC5213] deployment would benefit from a functionality where a Mobile Access Gateway (MAG) can dynamically discover a Local Mobility Anchor (LMA) for a Mobile Node (MN) attaching to a PMIPv6 domain. The purpose of the dynamic discovery functionality is to reduce the amount of static configuration in the MAG. Other drivers for the dynamic discovery of an LMA include LMA load balancing solutions and selecting an LMA based on desired services (i.e., allowing service-specific routing of traffic) [RFC5149]. This document describes several possible dynamic LMA discovery approaches and makes a recommendation of the preferred one.

The following list briefly introduces solution approaches that will be discussed in this document. The approaches discussed do not include all possible discovery mechanisms, but are limited to those considered to fit most simply into the PMIPv6 environment.

- LMA Address is retrieved from the Authentication, Authorization, and Accounting (AAA) infrastructure during the network access authentication procedure when the MN attaches to the MAG.
- LMA Fully Qualified Domain Name (FQDN) is retrieved from the AAA infrastructure during the network access authentication, followed by a Domain Name System (DNS) lookup.
- LMA FQDN is derived from the MN identity received from the lower layers during the network attachment, followed by a DNS lookup.
- LMA FQDN or IP address is received from the lower layers during the network attachment. The reception of an FQDN from the lower layers is followed by a DNS lookup.
- LMA FQDN is derived from the service selection indication received from lower layers during the network attachment, followed by a DNS lookup.

When an MN performs a handover from one MAG to another, the new MAG must use the same LMA that the old MAG was using. This is required for session continuity. The LMA discovery mechanism in the new MAG should be able to return the information of the same LMA that was being used by the old MAG. This document also discusses solutions for LMA discovery during a handover.

2. AAA-Based Discovery Solutions

This section presents an LMA discovery solution that requires a MAG to be connected to an AAA infrastructure (as described in [RFC5779], for instance). The AAA infrastructure is also assumed to be aware of PMIPv6. An MN attaching to a PMIPv6 domain is typically required to provide authentication for network access and to be authorized for mobility services before the MN is allowed to send or receive any IP packets or even complete its IP level configuration.

The AAA-based LMA discovery solution hooks into the network access authentication and authorization process. The MAG also has the role of a Network Access Server (NAS) at this step. While the MN is attaching to the network, the PMIPv6-related parameters are bootstrapped in parallel with authentication for the network access and authorization for the mobility services. The bootstrapping of PMIPv6 parameters involves the policy profile download over the AAA infrastructure to the MAG (see Appendix A of [RFC5213]).

2.1. Receiving the LMA Address during Network Access Authentication

After the MN has been successfully authenticated for network access and authorized for the mobility service, the MAG receives the LMA IP address from the AAA server over the AAA infrastructure. The LMA IP address information would be part of the AAA message that ends the successful authentication and authorization portion of the AAA exchange.

Once the MAG receives the LMA IP address, it sends a Proxy Binding Update (PBU) message for the newly authenticated and authorized MN. The MAG expects that the LMA returned by the AAA server is able to provide mobility session continuity for the MN, i.e., after a handover, the LMA would be the same one the MN already has a mobility session set up with.

2.2. Receiving the LMA FQDN during Network Access Authentication

This solution is similar to the procedure described in Section 2.1. The difference is that the MAG receives an FQDN of the LMA instead of the IP address(es). The MAG has to query the DNS infrastructure in order to resolve the FQDN to the LMA IP address(es).

The LMA FQDN might be a generic name for a PMIPv6 domain that resolves to one or more LMAs in the PMIPv6 domain. Alternatively, the LMA FQDN might be resolved to exactly one LMA within the PMIPv6 domain. The latter approach would obviously be useful if a new target MAG, after a handover, resolved the LMA FQDN to the LMA IP address where the MN mobility session is already located.

The procedures described in this section and in Section 2.1 may also be used together. For example, the AAA server might return a generic LMA FQDN during the MN's initial attachment, and once the LMA gets selected, return the LMA IP address during the subsequent attachments to other MAGs in the PMIPv6 domain. In order for this to work, the resolved and selected LMA IP address must be updated to the remote policy store. For example, the LMA could perform the policy store update using the AAA infrastructure once it receives the initial PBU from the MAG for the new mobility session.

3. Discovery Solutions Based on Data from Lower Layers

The following section discusses solutions where a MAG acquires information from layers below the IP layer. Based on this information, the MAG is able to determine which LMA to contact when the MN attaches to the MAG. The lower layers discussed here are not explicitly defined but include different radio access technologies and tunneling solutions such as an Internet Key Exchange version 2 (IKEv2) [RFC5996] IPsec tunnel [RFC4303].

3.1. Constructing the LMA FQDN from a Mobile Node Identity

A MAG acquires an MN identity from lower layers. The MAG can use the information embedded in the identity to construct a generic LMA FQDN (based on some pre-configured formatting rules) and then proceed to resolve the LMA IP address(es) using the DNS. Obviously, the MN identity must embed information that can be used to uniquely identify the entity hosting and operating the LMA for the MN. Examples of such MN identities are the International Mobile Subscriber Identity (IMSI) and the Globally Unique Temporary User Equipment Identity (GUTI) [3GPP.23.003]. These MN identities contain information that can uniquely identify the operator to whom the subscription belongs.

3.2. Receiving the LMA FQDN or IP Address from Lower Layers

The solution described here is similar to the solution discussed in Section 3.1. A MAG receives an LMA FQDN or an IP address from lower layers, for example, as a part of the normal lower-layer signaling when the MN attaches to the network. IKEv2 could be an existing example of such lower-layer signaling where IPsec is the "lower layer" for the MN [3GPP.24.302]. IKEv2 has an IKEv2 Identification - Responder (IDr) payload, which is used by the IKEv2 initiator (i.e., the MN in this case) to specify which of the responder's identities (i.e., the LMA in this case) it wants to talk to. And here the responder identity could be an FQDN or an IP address of the LMA (as the IKEv2 identification payload can be an IP address or an FQDN). Another existing example is the Access Point Name Information Element (APN IE) [3GPP.24.008] used in 3GPP radio network access signaling and capable of carrying an FQDN. However, in general, this means the MN is also the originator of the LMA information. The LMA information content as such can be transparent to the MN, meaning the MN does not associate the information with any LMA function.

3.3. Constructing the LMA FQDN from a Service Name

Some network access technologies (including tunneling solutions) allow the MN to signal the service name that identifies a particular service or the external network it wants to access [3GPP.24.302] [RFC5996]. If the MN-originated service name also embeds the information of the entity hosting the service, or the hosting information can be derived from other information available at the same time (e.g., see Section 3.1), then the MAG can construct a generic LMA FQDN (e.g., based on some pre-defined formatting rules) providing an access to the service or the external network. The pre-defined formatting rules [3GPP.23.003] are usually agreed on among operators that belong to the same inter-operator roaming consortium or by network infrastructure vendors defining an open networking system architecture.

Once the MAG has the FQDN, it can proceed to resolve the LMA IP address(es) using the DNS. An example of such a service or external network name is the Access Point Name (APN) [3GPP.23.003] that contains the information of the operator providing the access to the given service or the external network. For example, an FQDN for an "ims" APN could be "ims.apn.epc.mnc015.mcc234.3gppnetwork.org".

4. Handover Considerations

Whenever an MN moves and attaches to a new MAG in a PMIPv6 domain, all the MAGs that the MN attaches to should use the same LMA. If there is only one LMA per PMIPv6 domain, then there is no issue. If there is a context transfer mechanism available between the MAGs, then the new MAG knows the LMA information from the old MAG. Such a mechanism is described in [RFC5949]. If the MN-related context is not transferred between the MAGs, then a mechanism to deliver the current LMA information to the new MAG is required.

Relying on DNS during handovers is not generally a working solution if the PMIPv6 domain has more than one LMA, unless the DNS consistently assigns a specific LMA for each given MN. In most cases described in Section 3, where the MAG derives the LMA FQDN, there is no prior knowledge whether the LMA FQDN resolves to one or more LMA IP address(es) in the PMIPv6 domain. However, depending on the deployment and deployment-related regulations (such as inter-operator roaming consortium agreements), the situation might not be this desperate. For example, a MAG might be able to synthesize an LMA-specific FQDN (e.g., out of an MN identity or some other

service-specific parameters). Alternatively, the MAG could use (for example), an MN identity as an input to an algorithm that deterministically assigns the same LMA out of a pool of LMAs (assuming the MAG has, e.g., learned a group of LMA FQDNs via an SRV [RFC2782] query). These approaches would guarantee that DNS always returns the same LMA Address to the MAG.

Once the MN completes its initial attachment to a PMIPv6 domain, the information about the LMA that is selected to serve the MN is stored in the policy store (or the AAA server). The LMA information is conveyed to the policy store by the LMA after the initial attachment is completed [RFC5779]. Typically, AAA infrastructure is used for exchanging information between the LMA and the policy store.

When the MN moves and attaches to another MAG in the PMIPv6 domain, then the AAA server delivers the existing LMA information to the new MAG as part of the authentication and authorization procedure as described in Section 2.1.

5. Recommendations

This document discussed several solution approaches for a dynamic LMA discovery. All discussed solution approaches actually require additional functionality or infrastructure support that the base PMIPv6 specification [RFC5213] does not require.

Solutions in Section 3 all depend on lower layers being able to provide information that a MAG can then use to query the DNS and discover a suitable LMA. The capabilities of the lower layers and the interactions with them are generally out of scope of the IETF, and specific to a certain system and architecture.

Solutions in Section 2 depend on the existence of an AAA infrastructure, which is able to provide to a MAG either an LMA IP address or an LMA FQDN. While there can be system- and architecture-specific details regarding the AAA interactions and the use of DNS, the dynamic LMA discovery can be implemented in an access- and technology-agnostic manner, and work in the same way across heterogeneous environments. Therefore, using AAA-based LMA discovery solutions is recommended by this document. Furthermore, following the guidance in Section 4, Paragraph 4.1 of [RFC1958], the use of FQDNs should be preferred over IP addresses in the context of AAA-based LMA discovery solutions.

6. Security Considerations

The use of DNS for obtaining the IP address of a mobility agent carries certain security risks. These are explained in detail in Section 9.1 of [RFC5026]. However, the risks described in [RFC5026] are mitigated to a large extent in this document, since the MAG and the LMA belong to the same PMIPv6 domain. The DNS server that the MAG queries is also part of the same PMIPv6 domain. Even if the MAG obtains the IP address of a bogus LMA from a bogus DNS server, further harm is prevented since the MAG and the LMA should authenticate each other before exchanging PMIPv6 signaling messages. [RFC5213] specifies the use of IKEv2 between the MAG and the LMA to authenticate each other and set up IPsec security associations for protecting the PMIPv6 signaling messages.

The AAA infrastructure may be used to transport the LMA-discovery-related information between the MAG and the AAA server via one or more AAA brokers and/or AAA proxies. In this case, the MAG-to-AAA-server communication relies on the security properties of the intermediate AAA brokers and AAA proxies.

7. Acknowledgements

The authors would like to thank Julien Laganier, Christian Vogt, Ryuji Wakikawa, Frank Xia, Behcet Sarikaya, Charlie Perkins, Qin Wu, Jari Arkko, and Xiangsong Cui for their comments, extensive discussions, and suggestions on this document.

8. References

8.1. Normative References

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

8.2. Informative References

[3GPP.23.003]
3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 v10.0.0, December 2010.

[3GPP.24.008]
3GPP, "Mobile radio interface Layer 3 specification", 3GPP TS 24.008 v10.1.0, December 2010.

[3GPP.24.302]
3GPP, "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks", 3GPP TS 24.302 v10.2.0, December 2010.

[RFC1958] Carpenter, B., Ed., "Architectural Principles of the Internet", RFC 1958, June 1996.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC5026] Giaretta, G., Ed., Kempf, J., and V. Devarapalli, Ed., "Mobile IPv6 Bootstrapping in Split Scenario", RFC 5026, October 2007.

[RFC5149] Korhonen, J., Nilsson, U., and V. Devarapalli, "Service Selection for Mobile IPv6", RFC 5149, February 2008.

[RFC5779] Korhonen, J., Ed., Bournelle, J., Chowdhury, K., Muhanna, A., and U. Meyer, "Diameter Proxy Mobile IPv6: Mobile Access Gateway and Local Mobility Anchor Interaction with Diameter Server", RFC 5779, February 2010.

[RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

Authors' Addresses

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

EMail: jouni.nospam@gmail.com

Vijay Devarapalli
Vasona Networks

EMail: dvijay@gmail.com