NetLMM Working Group
Internet-Draft
Expires: February 1, 2008

M. Liebsch
NEC
C. Vogt
Ericsson
July 31, 2007

Context Transfer for Proxy MIPv6
draft-liebsch-netlmm-proxymip6ct-00.txt

Status of this Memo

Copyright Notice

Abstract

The IETF is specifying a protocol for network-based localized mobility management, which takes basic operation for registration, tunnel management and de-registration into account. This document specifies how the IETF's Context Transfer Protocol, which is specified in RFC 4067, can be used with protocols for network-based mobility management, taking proactive and reactive handover scenarios into account. The protocol Proxy Mobile IPv6 is suitable to support network-based mobility management, which is the reference protocol solution for the integration of the context transfer mechanisms in this document.

Table of Contents

1. Requirements notation

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].

2. Introduction

The NetLMM WG is specifying a protocol for network-based localized mobility management (NetLMM), taking basic support for registration, de-registration and handover into account in a first protocol release. The specification of extensions and optimization is for further study and subject for either being incorporated into future versions of the protocol or specified in separate documents. In scope of the base protocol specification is the set up and maintenance of a forwarding tunnel between an MN's Mobility Access Gateway (MAG) and its selected Local Mobility Anchor (LMA).

The protocol Proxy Mobile IPv6 [I-D.ietf-netlmm-proxymip6] is being designed to suit basic operation of network-based localized mobility management. According to [RFC4831], mobility management should not depend on mobility-related signaling from mobile nodes (MNs), such as location updates. However, it's considered as beneficial to support transfer of an MN's context between the MN's previous and new access routers in case the MN changes its point of attachment and this change implies a change in the MN's access router. Other mechanisms than receiving an explicit indication from the MN must be used to initiate the transfer of context between access routers.

This document specifies, how context transfer can be achieved in a Proxy MIPv6 enabled network. [RFC4067] is referred to as base and generic protocol operation between access routers to perform context transfer. The associated functional components for context transfer are embedded into the Proxy MIPv6 architecture and protocol operation to support context transfer efficiently by means of reusing Proxy MIPv6 protocol elements and event indications, without the need to rely on explicit indication from MNs.

This document first discusses different scenarios for context transfer in a Proxy-MIPv6 enabled network, taking context push and context pull operation, as well as support for proactive and reactive handover into account. Subsequently, the integrated protocol operation is described. Extensions to the Proxy MIPv6 protocol are described in case they are required to support some of the reference scenarios. If the integrated protocol operation relies on information, which is not available on the relevant network component, the source and means to retrieve such information is described.

3. Terminology and Functional Components

- MAG - Mobility Access Gateway. PMIPv6 functional component defined in [I-D.ietf-netlmm-proxymip6]. The MAG function is assumed to be located on the PMIPv6 domain's access routers.

- LMA - Local Mobility Anchor. PMIPv6 functional component defined in [I-D.ietf-netlmm-proxymip6].

- pAR - Previous Access Router. Equivalent to current access router. In a layer 3 handover situation, the access router which the mobile node is leaving.

- nAR - New Access Router. Equivalent to handover target access router. In a layer 3 handover situation, the access router towards which the mobile node is moving.

- pMAG - previous MAG. In a layer 3 handover situation, the MAG function located on the previous access router

- nMAG - new MAG. In a layer 3 handover situation, the MAG function located on the new access router.

- CT - Context Transfer. Means the transfer of any mobile node related context from the mobile's previous access router to its handover target access router.

- CR - Context Ready. Describes a state on an access router, indicating that the router is ready to activate a context as soon as it's available.

- CA - Context Activation. Describes a state on an access router, indicating that the router has the complete context received and activated.

- PHT - Proactive Handover Trigger. Describes an event on an access router, which indicates the preparation or execution of a proactive handover. Such indication provides further information about the handover target access router, such as its IP address or an unambiguous identifier.

- ATT - Attach. Describes an event on an access router, which indicates that a mobile node has attached to the router and has a fully functional layer-2 link established for bi-directional traffic. Such indication provides further information, which is required for the network-based mobility management protocol to operate.

4. Protocol Design

This section describes the integration of the IETF's Context Transfer protocol [RFC4067] with Proxy Mobile IPv6 [I-D.ietf-netlmm-proxymip6]. The reference architecture is described in Figure 1.

4.1. Reference Architecture

The reference architecture covers a mobile node (MN), which is attached to a local domain operating Proxy Mobile IPv6. The MN's Local Mobility Anchor (LMA) tracks the MN's location and maintains associated forwarding states towards the MN's current MAG. MAGs are assumed to be colocated with the domain's access routers. In case the MN changes its MAG due to a handover, the procedure implies that the MN detaches from its current access router, which implements the MN's previous MAG (pMAG) and attaches to a handover target access router, which implements the MN's new MAG (nMAG). The context transfer (CT) protocol is supposed to transfer the MN's context from its previous access router to its new access router. The reference architecture is illustrated in Figure 1.

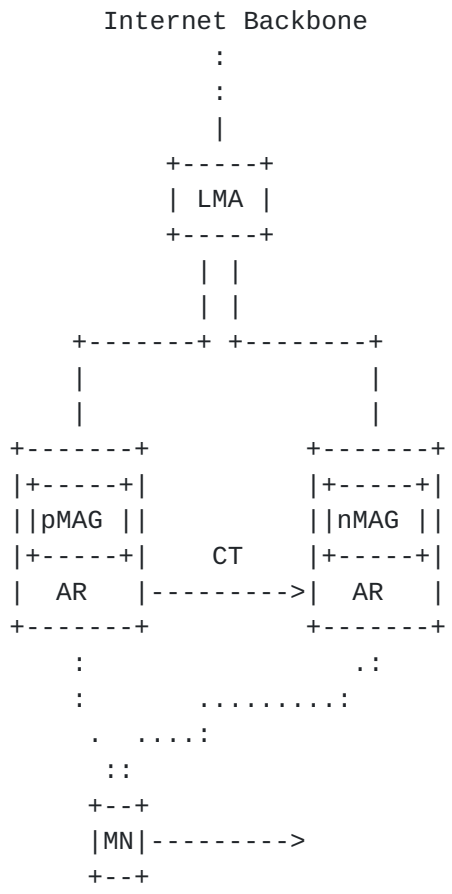

Figure 1: Reference architecture for context transfer in Proxy MIPv6.

Note: Within the context of the description in this document, pMAG always refers to the network component, which is the MN's previous access router, whereas nMAG refers to the MN's new access router.

4.2. Deployment Options

The integrated context transfer protocol leaves network operators deployment liberties along three orthogonal axes:

1. Context transfer may happen reactively or proactively.

2. Context transfer may be initiated by the pMAG or by the nMAG.

3. The initiating pMAG/nMAG may obtain the IP address of the correspondent nMAG/pMAG from any third entity.

Reactive context transfer is initiated either by the pMAG after the mobile node has detached from the pMAG, or by the nMAG after the

mobile node has attached to the nMAG. Proactive context transfer is initiated either by the pMAG before the mobile node detaches from the pMAG, or by the nMAG before the mobile node attaches to the nMAG.

Context transfer requires a trigger for the initiating MAG to indicate when the transfer should start. In case the context transfer is reactive, this trigger may be a notification from the link layer. If the context transfer happens proactively, the trigger is likely to originate from a handover prediction algorithm that runs on the initiating MAG.

Context transfer furthermore requires a "MAG resolution mechanism" through which the initiating MAG can obtain the IP address of the correspondent MAG. If the IP address of the correspondent MAG is to be obtained from the LMA, the MAG resolution mechanism may use options to Proxy Mobile IPv6 messages. The IP address of the correspondent MAG may also be obtained through a proprietary mechanism from the policy store, or via a local trigger. The nature of the MAG resolution mechanism determines whether the context transfer begins in parallel with the corresponding proxy binding update or afterwards.

5. Protocol Operation

This section describes the operation of the integrated context transfer protocol. The protocol operation is described for reactive as well as proactive handover and assumes the required information for context transfer is made available either through Proxy Mobile IPv6 signaling or by means of a local event, which provides the required information. The reactive handover can distinguish two different scenarios. In one scenario, all information required to operate Context Transfer on MAGs will be retrieved from the MN's LMA. A different scenario might support the provision of some required information from a local event, such as an ATTACH indication. The proactive handover requires the pMAG to learn about the network entity, which implements the MN's nMAG.

One general issue to be referred to is context deactivation and deletion on an MN's previous access router. It needs to be ensured that the context is not deleted before it has been completely transferred to the MN's new access router. This could be achieved by means of linking the lifetime of context information to the Proxy Mobile IPv6 binding update list (BUL) on a MAG. If the MN's entry expires in the BUL, the context can be deleted. This is somehow save, as a BUL entry is not explicitly deleted under control of an LMA, but has soft state characteristics, which expires. Deactivation of context on the pMAG should be coordinated by the individual component, which maintains the context.

5.1. Reactive Handover - Case 1

Figure 2 covers the integrated protocol operation for a reactive handover, where the nMAG can initiate context transfer only after the required information about the pMAG has been retrieved from the MN's LMA.

As the LMA is aware of the MN's pMAG, it can inform the nMAG about the pMAG's IP address. This information can be conveyed in a Mobility Option of the Proxy BACK message. Possible option is a pMAG_Address option, which carries the pMAG's IP address. Alternatively, the pMAG can be identified by means of an identifier, which can be resolved on the nMAG into the pMAG's IP address. For this purpose, a pMAG_ID option can be specified. The nMAG is ready to receive and activate context after the reception of the Proxy BACK. The context can be activated after context data has been transferred completely from the pMAG.

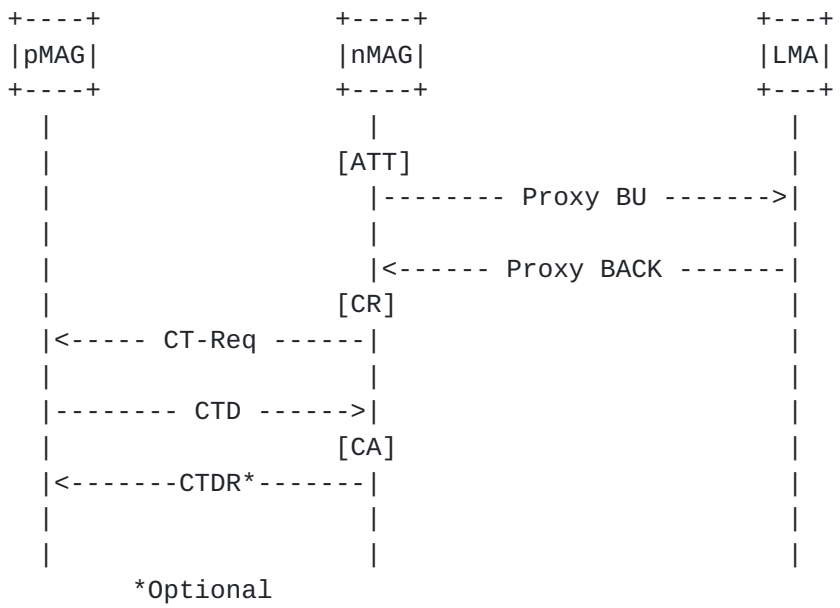

Figure 2: Reactive Handover - Case 1

5.2. Reactive Handover - Case 2

Figure 3 covers the integrated protocol operation for a reactive handover, where the nMAG retrieves information about the MN's pMAG through a local event, which also triggers the Proxy BU. This approach does not require any additional information from Proxy Mobile IPv6 operation. The context transfer can be performed in parallel to the Proxy Mobile IPv6 registration. The context can be activated on the nMAG after the reception of the context data.

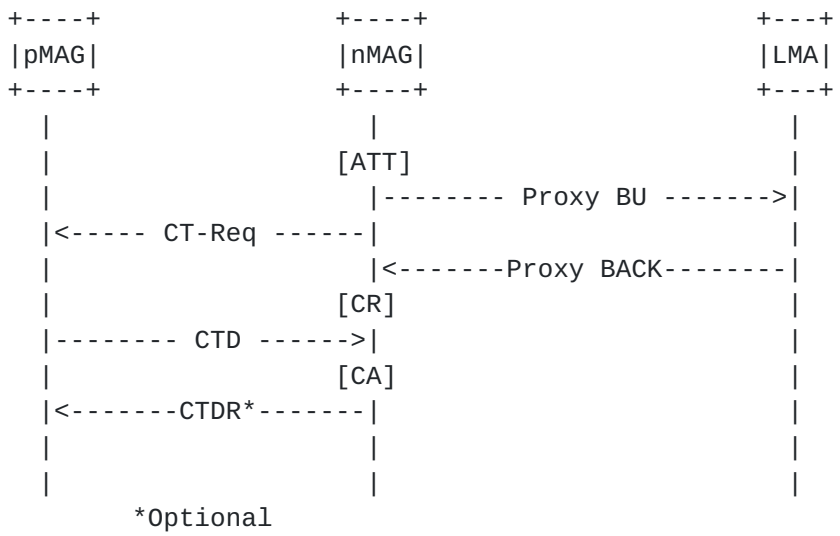

Figure 3: Reactive Handover - Case 2

5.3. Proactive Handover - Case 1

Figure 4 covers the integrated protocol operation for a proactive handover, where the pMAG can push an MN's context data to its target access router even before the MN attaches to the pMAG. The pMAG receives information about the MN's target access router through a local indication. This approach does not require any additional information from Proxy Mobile IPv6 operation. Advantageous of this approach is, that the nMAG can learn about the MN's LMA even before the MN attache MN attaches to the nMAG.

The nMAG is in this scenario permanently in CR mode for a set of potential pMAGs. In a typical deployment scenario, MAGs that may exchange contexts have preconfigured security associations. A permanent CR mode between those MAGs that can authenticate each other does not introduce new security risks. Garbage collection at the nMAG ensures that transferred context will be removed automatically in case the mobile node to which the context belongs never arrives at the nMAG.

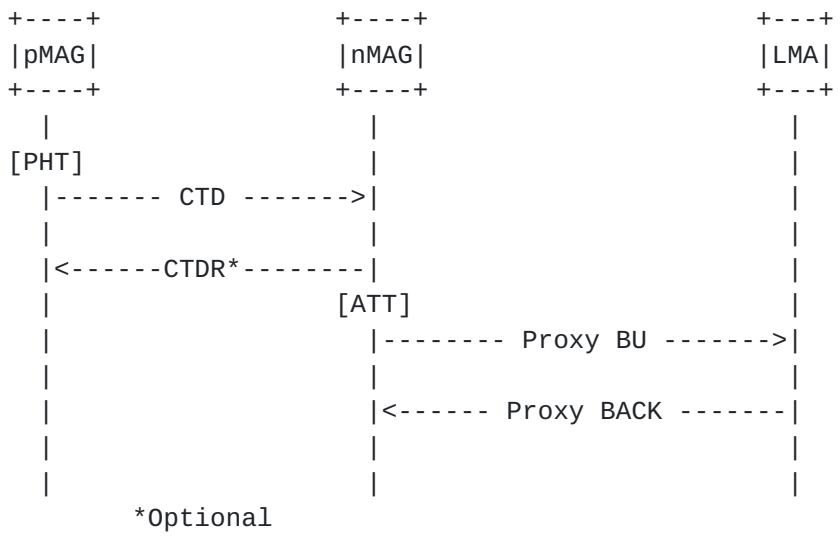

Figure 4: Proactive Handover - Case 1

5.4. Proactive Handover - Case 2

Figure 5 covers the integrated protocol operation for a proactive handover, where the nMAG retrieves information about the MN's pMAG through a local event. This approach does not require additional information from Proxy Mobile IPv6 operation. The context can be activated on the nMAG after the reception of the context data. The nMAG initiates the Proxy Mobile IPv6 registration once the mobile node attaches to it.

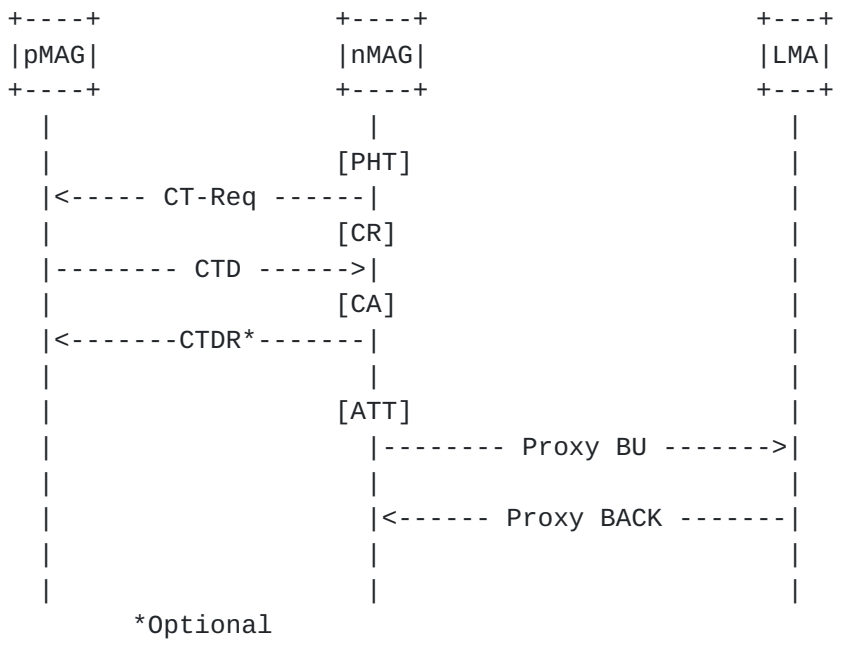

Figure 5: Proactive Handover - Case 2

6. Security Considerations

The integrated scenario as described in this document must meet the security requirements of the two individual protocol components, namely context transfer [RFC4067] and Proxy MIPv6 [I-D.ietf-netlmm-proxymip6].

Information about an MN's previous access router must be authenticated on the nMAG. If such information is retrieved from a policy store, the access router which implements the nMAG should share a security association with the policy store. Other mechanisms to protect such information must be applied in case there is no security association available between these network entities. The same applies for information about the new access router, which is used on the MN's pMAG to initiate context transfer in case of a proactive handover scenario.

7. IANA Considerations

This documents includes no request to IANA.

8. Contributors

This document comprises valuable contributions from Julien Abeille (abeille@netlab.nec.de).

9. Normative References

[I-D.ietf-netlmm-proxymip6]
Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-01 (work in progress), June 2007.

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

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4067] Loughney, J., Nakhjiri, M., Perkins, C., and R. Koodli, "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

[RFC4831] Kempf, J., "Goals for Network-Based Localized Mobility Management (NETLMM)", RFC 4831, April 2007.

Authors' Addresses

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

Phone: +49 6221 4342146
Email: liebsch@netlab.nec.de

Christian Vogt
Ericsson Research, NomadicLab
Hirsalantie 11
02420 Jorvas
Finland

Email: christian.vogt@ericsson.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).