Internet Engineering Task Force (IETF)
Request for Comments: 6279
Category: Informational
ISSN: 2070-1721

M. Liebsch, Ed.
NEC
S. Jeong
ETRI
Q. Wu
Huawei

June 2011

Proxy Mobile IPv6 (PMIPv6) Localized Routing Problem Statement

Abstract

Proxy Mobile IPv6 is the IETF Standard for network-based mobility management. In Proxy Mobile IPv6, mobile nodes are topologically anchored at a Local Mobility Anchor, which forwards all data for registered mobile nodes. The setup and maintenance of localized routing, which allows forwarding of data packets between two mobile nodes' Mobility Access Gateways without involvement of their Local Mobility Anchor in forwarding, is not considered. This document describes the problem space of localized routing in Proxy Mobile IPv6.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The IETF has specified Proxy Mobile IPv6 (PMIPv6) [RFC5213] as the base protocol for network-based localized mobility management (NetLMM). The scope of the base protocol covers the setup and maintenance of a tunnel between a Mobile Node's (MN's) Mobile Access Gateway (MAG) and its selected Local Mobility Anchor (LMA). Data packets will always traverse the MN's MAG and its LMA, irrespective of the location of the MN's remote communication endpoint. Even though an MN may be attached to the same MAG or a different MAG as its Correspondent Node (CN) within the same provider domain, packets being associated with their communication will traverse the MN's and the CN's LMA, which can be located topologically far away from the MN's and the CN's MAG or even in a separate provider domain.

[RFC5213] addresses the need to enable local routing of traffic between two nodes being attached to the same MAG, but does not specify the complete procedure to establish such localized routing state on the shared MAG.

The NetLMM Extensions (NetExt) Working Group has an objective to design a solution for localized routing in PMIPv6. This objective includes the specification of protocol messages and associated protocol operation between PMIPv6 components to support the setup of a direct routing path for data packets between the MN's and the CN's MAG, while both hosts receive mobility service according to the PMIPv6 protocol [RFC5213]. As a result of localized routing, these packets will be forwarded between the two associated MAGs without traversing the MN's and the CN's LMA(s). In cases where one or both nodes hand over to a different MAG, the localized routing protocol maintains the localized routing path. Relevant protocol interfaces may include the interface between associated MAGs, between a MAG and an LMA, and between LMAs. The setup of localized routing with CNs not registered with a PMIPv6 network is out of scope of the NetExt solution and this problem statement.

This document analyzes and discusses the problem space of always using the default route through two communicating mobile nodes' local mobility anchors. Furthermore, the problem space of enabling localized routing in PMIPv6 is analyzed and described, while different communication and mobility scenarios are taken into account. Based on the analysis, a list of key functional requirements is provided, serving as input to the design of the protocol solution.

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]. In addition, the following terms are used in the context of this problem statement:

- Mobile Node (MN): Mobile Node without IP mobility support, which is attached to a Mobile Access Gateway (MAG) and registered with a Local Mobility Anchor (LMA) according to the PMIPv6 specification [RFC5213].

o Correspondent Node (CN): Correspondent Node according to its definition in [RFC3775] with or without IP mobility support. The CN represents the communication peer of an MN that is attached to a MAG and registered with an LMA according to the PMIPv6 specification.

o Localized Routing: Result of signaling to set up routing states on relevant network entities to allow forwarding of data packets between an MN and a CN, which are attached to MAGs sharing the same provider domain, without intervention of the MN's LMA and the CN's LMA in data forwarding.

o Localized Routing States: Information for localized routing on relevant forwarding entities on the optimized data path between an MN and a CN. Such information includes route entries and tunnel endpoints and may include further information about the MN and the CN, such as the communicating nodes' Mobile Node Identifier and their assigned Home Network Prefix.

o Provider Domain: A network domain in which network components are administered by a single authority, e.g., the mobile operator.

3. Problem Statement for Localized Routing in PMIPv6

3.1. General Observation

The Mobile IPv6 (MIPv6) protocol [RFC3775] has built-in mechanisms for direct communication between an MN and a CN. Mechanisms for route optimization in MIPv6 cannot be directly applied in PMIPv6. Following the paradigm of PMIPv6, MNs are not involved in mobility signaling and hence cannot perform signaling to set up localized routes. Instead, the solution for localized routing must consider functions in the network to find out whether or not a localized route is to be used and then control the setup and maintenance of localized routing states accordingly without any assistance from the MN and the CN. In the case of communication between two nodes attached to the PMIPv6 network infrastructure and where each node is registered with an LMA, data packets between these two nodes will always traverse the responsible LMA(s). At least some deployments would benefit from having such communication localized, rather than having packets traverse the core network to the LMA(s). In the context of this document, such localized communication comprises offloading traffic from LMAs and establishing an optimized forwarding path between the two communication endpoints.

Localized routing is understood in [RFC5213] as optimization of traffic between an MN and a CN that are attached to an access link connected to the same MAG. In such a case, the MAG forwards traffic directly between the MN and the CN, assuming the MAG is enabled to support this feature (setting of the EnableMAGLocalRouting flag on the MAG) and the MN's LMA enforces this optimization. [RFC5213] does not specify how an LMA can enforce optimization for such local communication. Maintaining local forwarding between the MN and the regular IPv6 CN gets more complex in the case where the MN performs a handover to a different MAG. Such a use case is not considered in the specification and is out of scope of this problem statement. This document focuses on use cases where both nodes, the MN and the CN, are within a PMIPv6 network and served by an LMA in a domain of LMAs.

With localized routing, operators have the possibility of offloading traffic from LMAs and from the core network. Establishment of a direct path between the MN's and the CN's MAG can be beneficial for the following reasons: First, by limiting the communication to the access nodes, the data traffic traversing the MAG - LMA path (network) can be reduced. This is significant, considering that the transport network between the access and the core is often the bottleneck in terms of costs and performance. Second, there may be performance benefits for data flows between the MN and the CN in terms of delay and packet loss, especially when the MN and the CN are attached to the same MAG and the LMA is topologically far away from that MAG. Even when the MN and the CN are attached to different MAGs, there could be benefit in limiting the communication to the access network only, rather than traversing the transport network to the LMA. Furthermore, offloading traffic from the LMA by means of localized routing can improve scalability of the LMA, as it represents a bottleneck for traffic being forwarded by many MAGs.

3.2. Use Cases Analysis

This problem statement focuses on local communication between PMIPv6 managed nodes, which attach to MAGs sharing the same provider domain. The following list analyzes different use cases, which consider the existence of multiple LMAs. Figure 1 depicts a PMIPv6-based network with two mobility anchors. According to [RFC5213], the MN moves in the PMIPv6 domain being built by its LMA and MAG. The same applies to the CN, which moves in the PMIPv6 domain built by the CN's LMA and MAG. The analysis takes no assumption on whether the MN and the CN share the same PMIPv6 domain or not.

```
                              Internet Backbone
                             :                  :
                             +------------------+
                             |                  |
                          +----+              +----+
                          |LMA1|              |LMA2|
                          +----+              +----+
                             |                  |
                             |                  |
                        +----+------------------+----+
                        |                            |
                     +----+                       +----+
                     |MAG1|                       |MAG2|
                     +----+                       +----+
                     :    :                          :
                   +---+ +---+                     +---+
                   |MN | |CN1|                     |CN2|
                   +---+ +---+                     +---+
```

Figure 1: Reference Architecture for Localized Routing in PMIPv6

All "A" use cases below assume that both the MN and the CN are registered with an LMA according to the PMIPv6 protocol. Whereas MAG1 is always considered as the MN’s current Proxy Care-of Address, the CN can be either connected to the same MAG or to a different MAG or LMA as the MN. Accordingly, these topological differences are denoted as follows:

A[number of MAGs][number of LMAs]

A11: The MN and the CN (CN1) connect to the same MAG (MAG1) and are registered with the same LMA (LMA). The common MAG may forward data packets between the MN and the CN directly without forwarding any packet to the LMA. [RFC5213] addresses this use case, but does not specify the complete procedure to establish such localized routing state on the shared MAG.

A12: The MN and the CN (CN1) connect to the same MAG (MAG1) and are registered with different LMAs (LMA1 and LMA2). The common MAG may forward data packets between the MN and the CN directly without forwarding any packet to the LMAs. Following the policy of [RFC5213] and enforcement of the setup of a localized forwarding path, potential problems exist in the case where LMA1 and LMA2 differ in their policy to control the MAG.

A21: The CN (CN2) connects to a different MAG (MAG2) than the MN (MAG1), but the MN and the CN are registered with the same LMA (LMA1). The result of localized routing should be the existence of routing information at MAG1 and MAG2, which allows direct forwarding of packets between the MN's MAG1 and the CN's MAG2. As LMA1 is the common anchor for the MN and the CN and maintains location information for both nodes, no major race condition and instability in updating the states for localized routing is expected.

A22: The CN (CN2) connects to a different MAG (MAG2) and a different LMA (LMA2) than the MN (MAG1, LMA1). The result of localized routing should be the existence of routing information at MAG1 and MAG2, which allows direct forwarding of packets between the MN's MAG1 and the CN's MAG2. As the location information of the CN and the MN is maintained at different LMAs, both LMAs need to be involved in the procedure to set up localized routing. In the case of a handover of the MN and/or the CN to a different MAG, non-synchronized control of updating the states for localized routing may result in race conditions, superfluous signaling, and packet loss.

The following list summarizes general problems with setting up and maintaining localized routing between an MN and a CN. In the context of this problem statement, the MN and the CN are always assumed to be registered at an LMA according to the PMIPv6 protocol [RFC5213].

o MNs do not participate in mobility management and hence cannot perform binding registration at a CN on their own. Rather, entities in the network infrastructure must take over the role of MNs to set up and maintain a direct route. Accordingly, a solution for localized routing in PMIPv6 must specify protocol operation between relevant network components, such as between a MAG and an LMA, to enable localized routing for data traffic without traversing the MN's and the CN's LMA(s).

o In the case where the MN and the CN are both registered with different LMAs according to the PMIPv6 protocol, relevant information for the setup of a localized routing path, such as the current MAG of the MN and the CN, is distributed between these LMAs. This may complicate the setup and stable maintenance of states enabling localized routing.

o In the case where localized routing between an MN and a CN has been successfully set up and both nodes move and attach to a new access router simultaneously, signaling the new location and maintenance of states for localized routing at relevant routers may run into a race condition situation. This can happen in the case where coordination of signaling for localized routing and provisioning of relevant state information is distributed between different network entities, e.g., different LMAs. In such a case, as a result of the MN's handover, updated information about the MN's location may arrive at the CN's previous MAG, while the CN has already moved to a new MAG. The same applies to the other direction, where the system may update the MN's previous MAG about the CN's new location, while the MN has moved to a new MAG in the meantime. The protocol solution must deal with such exceptional handover cases efficiently to avoid or resolve such problems.

3.3. IPv4 Considerations

According to [RFC5844], the basic configuration requirements for supporting IPv4 in PMIPv6 are that LMAs and MAGs are both IPv4 and IPv6 enabled. Also, LMAs and MAGs must have a globally unique IPv6 address configured, irrespective of enabled support for IPv6 routing between these components. This requirement should also apply to configuration requirements of localized routing.

Additional issues emerge when localized routing is considered for PMIPv6 with IPv4 support. These can be classified into two general groups: issues with localized routing between an MN's and a CN's IPv4 Home Addresses, and transport plane issues. The following subsections analyze these two groups.

3.3.1. Localized Routing for Communication between IPv4 Home Addresses

In the case where an LMA and a MAG hold a registration to support IPv4 Home Address mobility for an MN, the MAG and the LMA must support appropriate encapsulation of IPv4 packets. To enable localized routing, the MN's MAG must encapsulate and forward routing path optimized packets to the CN's MAG and needs to ensure that the chosen encapsulation mode is supported by the correspondent MAG. Incompatibility in a selected encapsulation mode causes failure in setting up a localized route.

When localized routing is used for IPv4 traffic, the conceptual data structures on associated MAGs must be augmented with appropriate parameters for forwarding localized traffic. MAGs may need to maintain a routing state for each MN-CN-pair and make routing decisions for uplink traffic based on the packet's complete IPv4 source and destination address. Hence, conceptual data structures to handle states for localized routes need to comprise this address tuple for unique identification.

As a known constraint, IPv4 addresses of two nodes that hold addresses from a private address space may overlap. To uniquely identify both nodes, the IPv4 address of the MN and the CN must not overlap. To cope with overlapping address spaces, the localized routing solution could use additional mechanisms to tag and uniquely identify the MN and the CN.

3.3.2. IPv4 Transport Network Considerations

The transport network between the LMA and the MAG may be based on IPv6 or IPv4. Deployments may ensure that the same transport mechanism (i.e., IPv6 or IPv4) is used for operational consistency. Similar to the encapsulation requirement stated in the previous section, the IP version used for localized routing is also assumed, by configuration, to be consistent across all MAGs within the associated provider domain. The design of optional mechanisms for negotiating the IP version to use as well as the encapsulation mode to use are outside the scope of the NetExt WG's solution for localized routing.

4. Functional Requirements for Localized Routing

Several tasks need to be performed by the network infrastructure components before relevant information for such direct communication is discovered and associated states for localized routing can be set up. The following list summarizes some key functions that need to be performed by the PMIPv6-enabled network infrastructure to substitute mobile nodes in setting up a direct route.

- o Detection of the possibility to perform localized routing. This function includes looking at a data packet's source and destination address.

- o Initiation of a procedure that sets up a localized routing path.

- o Discovery of stateful entities (i.e., the LMA(s) and/or the MAG(s)) that maintain and can provide relevant information needed to set up a localized routing path. Such information may include the routable address of an LMA or MAG, where one or both mobile nodes are connected to and registered with that LMA or MAG.

- o Control in setting up and maintaining (e.g., during handover) the localized routing path. Control is also needed to terminate the use of a localized routing path and to delete associated states, whereas a trigger for the termination may come from a non-PMIPv6-related component.

- o Enforcement of administrative policy rules to localized routing. Such policies allow operators to have further control of the setup of a localized route and enable the possibility to disallow localized routing, for example, to ensure that traffic traverses charging-related functions on the LMA. Explicit authorization of localized routing is, for example, discussed in [PMIP6-LR]. As a further example, mobile-node- and operator-specific policy rules can be established on PMIPv6 components during PMIPv6 bootstrapping according to [RFC5779].

5. Roaming Considerations

Figure 2 shows PMIPv6 roaming cases where PMIPv6 components (e.g., LMAs, MAGs) tied by the MN and the CN may be distributed between different provider domains (i.e., domain A, B, C) and the MN and/or CN moves from one provider domain to another one. In order to support localized routing when roaming occurs, it is required that MAGs to which the MN and CN connect be within the same provider domain, and each MAG has a security relationship with the corresponding LMA, which maintains the registration of the MN or the CN, respectively.

According to the roaming model as depicted in Figure 2, the MN’s PMIPv6 domain is characterized by its MAG (MAG1/MAG1’) and its LMA (LMA1), whereas the CN’s PMIPv6 domain is characterized by the CN’s MAG (MAG2/MAG2’) and its LMA (LMA2/LMA2’). A solution for localized routing cannot take any assumption about whether or not the MN and CN share the same PMIPv6 domain; hence, MAG1/MAG1’ may not share a security association with LMA2/LMA2’, and MAG2/MAG2’ may not share a security association with LMA1, respectively.

It is not required that LMAs, which hold the registration for the MN and the CN, respectively, be part of the same provider domain as the MAGs where the MN and CN attach. When the MN’s MAG and LMA belong to different provider domains (A and C), localized routing is subject to policy governing the service level agreements between these domains. The same applies to the provider domains that provide the CN’s MAG and LMA. Based on the above requirements, four PMIPv6 roaming and non-roaming cases can be taken into account.

- o Case 1: The MN’s MAG (MAG1), the CN’s MAG (MAG2), the MN’s LMA (LMA1), and the CN’s LMA (LMA2) are located in the same provider domain A.

- o Case 2: The MN’s MAG (MAG1), the CN’s MAG (MAG2), and the MN’s LMA (LMA1) are located in the same domain A, while the CN’s LMA (LMA2’) is located in provider domain B.

o Case 3: The MN's MAG (MAG1') and the CN's MAG (MAG2') are located in domain C, while the MN's LMA (LMA1) and the CN's LMA (LMA2) are located in provider domain A.

o Case 4: The MN's MAG (MAG1') and the CN's MAG (MAG2') are located in provider domain C, while the MN's LMA (LMA1) is located in provider domain A and the CN's LMA (LMA2') is located in provider domain B.

In these roaming cases, the MN can be allowed to roam within its domain (e.g., the MN's home domain in which the MN's LMA is located) or over different domains (e.g., the MN moves from its home domain to a visited domain). During mobility, the CN and MN should remain attached to MAGs of the same provider domain to maintain efficient routing of traffic between their MAGs.

```
                                            |
          +------+       +------+           |       +------+
          |LMA1  |       |LMA2  |           |       |LMA2'|
          +------+       +------+           |       +------+
                                            |
                                            |
                                            |
                                            |
          +------+       +------+           |
          |MAG1  |       |MAG2  |           |
          +------+       +------+           |
                                            |
                                            |
                 Provider Domain A          |  Provider Domain B
     ---------------------------------------+-------------------------------
                                Provider Domain C

                             +------+        +------+
                             |MAG1'|        |MAG2'|
                             +------+        +------+
```

Figure 2: PMIPv6 Roaming Cases Considered for Localized Routing

6. Security Considerations

A protocol solution for localized routing in a PMIPv6 network must counter unauthorized change of a routing path. In particular, the control plane for localized routing must preclude the blocking or hijacking of mobile nodes' traffic by malicious or compromised network components. A security solution must support suitable mechanisms for authentication of control plane components of the localized routing functional architecture for both roaming and non-roaming scenarios. Any possibility for Internet hosts to interfere with the localized routing procedure in a malicious manner must be precluded.

Since network entities other than MNs and CNs perform signaling to set up localized routing, the MIPv6 return routability test [RFC3775] is not suitable to authenticate associated signaling messages in PMIPv6. Solutions for localized routing in PMIPv6 need to mitigate, or to provide sufficient defense against, possible security threats. When PMIPv6 participants are administered within the same domain, infrastructure-based authorization mechanisms, such as IPsec, may be usable to protect signaling for localized routing.

Existing security associations according to [RFC5213] can be re-used to protect signaling for localized routing on the interface between a MAG and an LMA. In the case where a protocol solution for localized routing in PMIPv6 relies on protocol operation between MAGs, means for protection of signaling between these MAGs must be provided. The same applies for signaling on a possible protocol interface between two LMAs of the same domain.

7. Acknowledgments

Many aspects of the problem space for route optimization in PMIPv6 have been discussed in the context of a PMIPv6 Route Optimization Design Goals document, which was submitted to the NetLMM WG in November 2007. This group of contributors includes Sangjin Jeong, Christian Vogt, Ryuji Wakikawa, Marco Liebsch, Behcet Sarikaya, Shinta Sugimoto, Long Le, Alice Qinxia, and Jaehwoon Lee. Many thanks to Rajeev Koodli for his comments about the structure and scope of this problem statement for the NetExt WG.

This problem statement reflects the results of the discussion in the NetExt group. Many thanks to Hidetoshi Yokota, Carlos Bernardos, Ashutosh Dutta, Sri Gundavelli, Mohana Jeyatharan, Jouni Korhonen, Glen Zorn, Dirk von Hugo, Frank Xia, Xiangsong Cui, and Basavaraj Patil for their comments and support to improve the quality of the problem statement.

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., Ed., 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

[PMIP6-LR] Zorn, G., Wu, Q., Liebsch, M., and J. Korhonen, "Diameter Support for Proxy Mobile IPv6 Localized Routing", Work in Progress, May 2011.

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

[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.

Authors' Addresses

Marco Liebsch (editor)
NEC Laboratories Europe
NEC Europe Ltd.
Kurfuersten-Anlage 36
69115 Heidelberg
Germany

Phone: +49 6221 4342146
EMail: liebsch@neclab.eu

Sangjin Jeong
ETRI
218 Gajeongno, Yuseong
Daejeon 305-700
Korea

Phone: +82 42 860 1877
EMail: sjjeong@etri.re.kr

Qin Wu
Huawei Technologies Co., Ltd
101 Software Avenue, Yuhua District
Nanjing 210012
China

Phone: +86 25 56623633
EMail: sunseawq@huawei.com