Abstract

Proxy Mobile IPv6 (PMIPv6) is the network-based mobility management protocol where access network supports the mobility of a mobile node on behalf of the MN. In PMIPv6, the location information of the MN should be registered to Localized Mobility Anchor and communication must be established via the LMA. Therefore, the performance can be degraded due to traffic concentration and congestion possibility. One method to overcome the above problems is to exploit the distributed mobility management (DMM) mechanism to distribute the LMA function to all access routers within the PMIPv6 domain. This letter proposes the fully distributed mobility management mechanism in PMIPv6-based network. In this mechanism, there is no need for the location management function to register the location of the MN. Therefore, the performance is not degraded due to the overhead to query the location of the MN.

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 November 20, 2014.
Copyright Notice

Copyright (c) 2014 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 used in this document .........................4
   2.2. Terminology ............................................4
3. Protocol Operation..............................................5
4. Security Considerations........................................7
5. IANA Considerations..............................................7
6. References......................................................7
Author’s Address...................................................7
1. Introduction

Mobile IPv6 (MIPv6) defines a protocol that allows a mobile node (MN) to maintain connectivity with a correspondent node (CN) within the Internet while changing its point of attachment [1]. In MIPv6, an MN is assigned with an IPv6 address as the home address, and a home agent (HA) is defined as the mobility agent that has the same network address as that of the home address of the MN. Whenever an MN visits a foreign network, it is assigned with a care-of address (CoA) and registers its home address and the CoA to its HA by using the Binding Update (BU) message. After that, the tunnel is established between the MN and the HA, and the MN can communicate with any host within the Internet. MIPv6 is considered as the host-based mobility management protocol that an MN initiates the operation defined in the MIPv6 whenever the MN detects that it changes the point of attachment.

Even though the MIPv6 is defined as the Internet standard, the overhead to run the MIPv6 in an MN is not small. Proxy MIPv6 (PMIPv6) is standardized as an Internet standard where access networks within the PMIPv6 domain support the mobility of an MN on behalf of the MN [2]. In PMIPv6, a Mobile Access Gateway (MAG) is defined to support the mobility of an MN. The MAG acts as the default gateway of the access link to which an MN is connected. Moreover, the Localized Mobility Anchor (LMA) is defined as the home agent of an MN within the PMIPv6 domain. In PMIPv6, every MAG advertises the same network prefix to an MN so that the MN considers that it connects to the same network while the MN moves one network to another. The MAG that the MN connects transmits the Proxy BU (PBU) message with its address (that is, Proxy-CoA) and the information of the MN to the LMA and establishes the tunnel between itself and the LMA in order for the MN to maintain the pre-established session.

MIPv6 and PMIPv6 use one centralized agent such as HA and LMA, respectively. Such centralized functions have several problems such as single-node failure, congestion possibility, scalability issues and non-optimal routes [3]. One method to resolve such problems is to use the dynamic mobility management (DMM) mechanism to distribute mobile agent function to access routers [4]. Especially, in PMIPv6, access networks need to support the mobility of MNs in order for an MN to use the pre-assigned address and to maintain the pre-established session. One method to provide the DMM in PMIPv6 domain is to distribute the LMA function to every MAG. Here, a MAG that an MN enters the PMIPv6 domain and firstly connects becomes the LMA for the MN. Moreover, the MAG becomes the default gateway for the MN.

That is, LMA function can be distributed because different MNs firstly connect to different MAGs and different MAGs become different LMAs for different MNs. Moreover, because the access router to which
an MN firstly connects provides the MAG and LMA functions, optimal path can be established between the MN and a CN. However, PMIPv6 domain should support the mobility of an MN on behalf of the MN. When an MN moves one network to another, a new access router that the MN moves and connects should know (1) whether the MN firstly enters the PMIPv6 domain and (2) the address information of the LMA for the MN when the access router knows that the MN moves from another network. One way to do it is to use the partial DMM mechanism [5-7]. The partial DMM mechanism in PMIPv6 environment defines a Location Management Function (LMF). A MAG that an MN firstly enters the PMIPv6 domain and firstly connects becomes the LMA for the MN. The LMA registers its address and MN’s ID with the LMF. When the MN moves and connects to a different MAG, the MAG queries the address information of the MN and LMA, and establishes the tunnel with the LMA. After that, the MN can continue to communicate any host within the Internet. However, there can also occur single-node failure problem. Moreover, control messages to query the LMA address information for MNs are concentrated to the LMF, which occurs the congestion possibility.

In this draft, we propose the fully distributed mobility management mechanism. The proposed mechanism does not need the control function such as LMF. Therefore, it does not occur the single-node failure problem. Moreover, the performance degradation does not occur due to the overhead to register and query the LMA address information for an MN. Packet loss and/or packet’s out-of-order transmission can be avoided by using the proposed mechanism.

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 [8].

2.2 Terminology

TBD.

3. Protocol Operation
The message exchange procedure between network entities to provide fully distributed mobility management in PMIPv6 environment proposed in this draft is presented in Figure 1. A network prefix "PREF" is allocated to the PMIPv6 domain. However, a different sub-network prefix belonging to the same network prefix "PREF" is allocated to a different MAG in PMIPv6 domain. In the example of Fig. 1, a sub-network prefix "PREF1" belonging to "PREF" is allocated to MAG1 and a different sub-network prefix "PREF2" belonging to the same "PREF" is allocated to MAG2. Even though a different sub-network prefix is allocated to a different MAG, all MAGs advertise the same network prefix "PREF" through the interfaces providing PMIPv6 service.

When an MN firstly enters the PMIPv6 domain and connects to a MAG (say, MAG1), MAG1 transmits to the MN a Router Advertisement (RA) message by setting "M (Managed address configuration)" flag in order to configure an address to the MN by using the stateful address configuration method [9]. The network prefix "PREF" is set to the prefix option information field in the RA message. The MN receiving the RA message transmits the dynamic host configuration protocol (DHCP) request message to the MAG1 [10]. The MAG1 considers that the MN firstly connects to the PMIPv6 domain and transmits the
DHCP response message containing an address belonging to the "PREF1" to the MN. The MN sets the address contained in the DHCP response message to its interface. After that, the MN can communicate to a CN within the Internet.

When the MN moves MAG1 to MAG2 while communicating with a CN, the MAG1 begins to perform the LMA function for the MN and stores packets sent from the CN into the buffer. The MAG1 stores the MM’s information into its Binding Cache Entry (BCE). When the MN connects to MAG2, the MAG2 transmits the RA message containing network prefix set to "PREF" to the MN. The MN receiving the RA message considers that it connects to the same network by using the "PREF" network prefix in prefix information option of RA message. It continues to use the address configured previously and transmits IP packets as usual. MAG2 checks the first packet transmitted by the MN. If the first packet contains the DHCP request packet, then MAG2 considers that the MN firstly connects to the PMIPv6 domain. Otherwise, MAG2 considers that the MN moves from another MAG area and creates the Binding Update List (BUL) for the MN. And then, MAG2 transmits the Distributed Proxy Binding Update (DPBU) message. The source address of the packet containing the DPBU message is set to the address of the MAG2 (say, Proxy-CoA2) and the destination address is set to the address of the MN. Here, MAG2 can know the address of the MN by using the source address of the IP packet sent by the MN. Moreover, MAG2 stores packets sent by the MN. DPBU message is transmitted to the MAG1 through the Internet topologically correct routing path. MAG1 receiving the DPBU message stores the Proxy-CoA2 address to its BCE for the MN, establishes the tunnel with MAG2, and transmits the Distributed Proxy Binding Acknowledgement (DPBA) message to MAG2. The source and destination addresses of the packet containing the DPBA message are set to the address of MAG1 (say, Proxy-CoA1) and Proxy-CoA2, respectively. The DPBA message contains the address of the MN in its option field. MAG2 receiving the PBA message stores the Proxy-CoA1 address to its BUL and establishes the tunnel with MAG1. And then, MAG1 transmits the packets stored in the buffer to MAG2, and MAG2 would the received packets to the MN. After that, the MN continues to communicate with the CN.

Packets sent from MAG1 to MAG2 might be lost if the MN moves from MAG2 to another MAG (MAG3 for example in this draft). It is because MAG1 cannot know the fact that the MN moves and connects to MAG3. In order to avoid the packet loss, when MAG2 knows to disconnect to the MN, MAG2 transmits the Distributed Proxy Binding Release Update (DPBRU) message to MAG1. Moreover, MAG2 transmits packets for the MN to MAG1 again. When MAG1 receives the DPBRU message, MAG1 transmits FLUSH message to the MAG2 and stores packets sent from the CN in its buffer. MAG2 having received the FLUSH message considers that the message is the final packet sent from the MAG1 and retransmits the FLUSH message. And then, MAG2 removes the entry related the MN in the BUL. MAG1 having received the flush message having sent from MAG2.
considers that the message is the final packet sent from MAG2. MAG1 transmits the Distributed Proxy Binding Release Acknowledgement (DPBRA) message to MAG2. When MAG1 receives the DPBU message from MAG3, MAG1 transmits the DPBA message to MAG3, update its BCE related to the MN, transmits the stored packets sent from MAG2, and then transmits packets sent from the CN.

4. Security Considerations

TBD

5. IANA Considerations

TBD

6. References


Author’s Address

Jaehwoon Lee
Dongguk University
26, 3-ga Pil-dong, Chung-gu
Seoul 100-715, KOREA
Email: jaehwoon@dongguk.edu

Younghan Kim
Soongsil University
369, Sangdo-ro, Dongjak-gu,
Seoul 156-743, Korea
Email: younghak@ssu.ac.kr