Service Flow Identifier in Proxy Mobile IPv6
draft-hui-netext-service-flow-identifier-03.txt

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on Jan 2011.

Copyright Notice

Copyright (c) 2009 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.
Abstract

This document proposes extensions to Proxy Mobile IPv6 that allows service flow identification and binding, and PMIP tunnels will be set up based on the service flow granularity. Therefore, multiple service flows of the mobile node can be separately controlled, e.g. QoS, charging, traffic control, and provides the precondition of flow mobility among multiple interfaces of the mobile node.
Table of Contents

1. Introduction .................................................. 4
2. Protocol Operation ........................................... 5
3. Message Formats ................................................. 7
   3.1. Service Flow Identifier option .......................... 7
   3.2. Service Flow Description option ......................... 8
4. Scenario ................................................................... 10
5. Mobility Access Gateway Operation ............................ 12
   5.1. Binding Update List extensions ............................ 12
   5.2. Service Flow Proxy Binding Update Operation .......... 12
   5.3. Data Forwarding Rules ....................................... 12
6. Local Mobility Anchor Operation ................................ 14
   6.1. Binding Cache extensions ................................... 14
   6.2. Service Flow Proxy Binding Acknowledge Operation ... 14
   6.3. Data Forwarding Considerations ........................... 14
7. Security Considerations ........................................ 16
8. IANA Considerations ............................................. 17
9. References ................................................................ 18
   9.1. Normative References ....................................... 18
   9.2. Informative References ..................................... 18
Author’s Addresses .................................................. 19
1. Introduction

Proxy Mobile IPv6 is a network-based local mobility management protocol which binds the home network prefix(es) assigned to a given interface of a mobile node to its current care-of address (Proxy-CoA). The mobile access gateway performs the proxy binding update with the local mobility anchor and does the mobility management on behalf of the mobile node attached to the network. Details of protocol operation and related terminologies are given in RFC 5213 [1].

PMIPv6 is based on the MIPv6 [2] that is a host-based global mobility management protocol. It reuses the home agent functionality and the message formats used in mobility signaling of MIPv6. In draft-ietf-mext-flow-binding [3], MIPv6 is extended to allow the binding of a particular flow to a care-of address without affecting other flows using the same home address. Therefore, each flow of the mobile node’s multiple interfaces can be separately forwarded based on the flow identifier in the binding update.

Current PMIPv6 protocol is host granularity basis. There is only one tunnel between a pair of LMA and MAG, so the network side cannot distinguish the different payload in the tunnel, and the operator can’t do service control consequently. To enable the traffic control, charging and QoS control per service flow basis in PMIPv6 domain, PMIPv6 should be enhanced to achieve flow granularity control. To support the service flow proxy binding update operation, each service flow of the mobile node can be forwarded and controlled separately, which is mapped to one PMIPv6 tunnel, one BCE/BULE and one pair of GRE Keys.

In this document, a new Service Flow Identifier option is defined to carry the service flow identifier and service flow attributes in the Proxy Binding Update and Acknowledgement message. Hence, the mobile access gateway can bind mobile node’s each service flow to its home network prefix, respectively. Therefore, the mobile node’s multiple service flows can be separately controlled based on the service flow identifier. E.g. charging and QoS control can be implemented per each service basis, as different charging criteria are applicable to the mobile node’s different service flows.
2. Protocol Operation

```
+-----+    +-----+    +-----+
| MN  |    | MAG |    | LMA |
+-----+    +-----+    +-----+
```

1. <--------RS/RA------> <--------PBU/PBA------>
   ==== Bi-Dir Tunnel ==== (for Mobile node)

2. ----Start a New SF---->

3. """
   """

4. <--------PBA (SF) -------->

5. """
   """

6. <-------- data --------> ======== data ========

---

Figure 1  Service Flow (SF) Proxy Binding Update

Figure 1 shows the signaling call flow using the PMIPv6 extension when the mobile node starts a new service flow.

1. The bi-directional tunnel between the mobile access gateway and the local mobility anchor is set up for the mobile node, based on the standard attach procedure in PMIPv6, specified in RFC 5213 [1].

2. When a new service flow of the mobile node is started (e.g. launch a new service), the data packet of this service will be routed to the mobile access gateway.

3. The mobile access gateway analyzes the received data packet (this analysis mechanism can be achieved in several ways which is out of scope of this draft), catching the corresponding packet filter attributes, and generates a unique service flow identifier and the service flow description option for this service flow. Then it sends a Proxy Binding Update message to the mobile node’s local mobility anchor for updating the service flow binding information including the service flow identifier option and the assigned downlink GRE Key for this binding.

4. Upon receiving the Proxy Binding Update message from the mobile access gateway, the local mobility anchor will first check the
validity of the Proxy Binding Update message and assure the uniqueness of the SFID value. If the proxy binding update is accepted, it will return a Proxy Binding Acknowledgement message including the service flow identifier option and the uplink GRE Key for this binding. It also creates the new binding cache entry that including home network prefix(es) of the mobile node, service flow identifier, packet filter attributes, and the assigned uplink and downlink GRE Key for this service flow binding. A new BCE/BULE and a new pair of GRE Keys are assigned for each service flow.

5. The new bi-directional tunnel for this specific service flow between the mobile access gateway and the local mobility anchor is set up to forward the corresponding data packets.

6. When the data packet of this service flow is routed to the mobile access gateway, it will check the binding update list and attain the uplink GRE Key. And then it encapsulates and forwards the data packet to the mobile node’s local mobility anchor.

Hence, multiple service flows of the mobile node can be separately controlled based on the service flow identifier in the service flow identifier option of the Proxy Binding Update message, e.g. different charging criteria can be adapted to mobile node’s each service flow.
3. Message Formats

This section introduces extensions to PMIPv6 that are necessary for supporting the service flow binding mechanism.

3.1. Service Flow Identifier option

The Service Flow Identifier option is a variable-length option, included in the Proxy Binding Update and Acknowledgement message. It must come with the Service Flow Description option that contains the packet filter attributes of the service flow.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Option Type   |  Option Len   |   Status      | PRO   |Reserved|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Service Flow Identifier      |              Reserved          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                Service Flow Description option                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2 The Service Flow Identifier option

**Status**

This field indicates the success or failure of the service flow binding operation for the particular service flow in the option. This field is only relevant when included in the Proxy Binding Acknowledgement message and must be ignored in the Proxy Binding Update message.

**Service Flow Identifier**

It is a 16-bit unsigned integer, including the unique identifier within the LMA scope. However, its length can also be implementation dependent.

The service flow identifier is used to name the different service flows.

**PRO**

A 4-bit field that describes the operation that the receiver has to perform, e.g. adding, modifying or deleting the option. The following values are reserved for the PRO field:
0 Add a service flow binding
1 Modify a service flow binding
2 Delete a service flow binding

Service Flow Description option

A variable-length option that contains the valid packet filter attributes combinations of the particular service flow, e.g. Port.

3.2. Service Flow Description option

The service flow description option is a variable-length option, included in the service flow identifier option. It contains the three kinds of valid packet filter attribute combination of the service flow which are defined in 3GPP TS23.060 [5] and TS23.203 [6].

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Option Type   | Option Len    |          Reserved             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type  |             Service Flow Description               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3 The Service Flow Description option

Type

This field indicates one of the three kinds of the valid packet filter attribute combination of the particular service flow.

Service Flow Description

The detailed binary encoding of the service flow description field could follow the defined binary traffic selector in draft-ietf-mext-binary-ts [7]. The following values are reserved for the Type and Service Flow Description field:

0 <destination address, source port range, destination port range, protocol ID of the protocol above IP, Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask>

1 <destination address, protocol ID of the protocol above IP, Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask, the IPSec Security Parameter Index (SPI)>
2 <destination address, Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask, the Flow Label (IPv6)>
4. Scenario

This section introduces a use case of multiple service flows binding.

![Diagram of LMA Binding Cache and PMIPv6 domain with two service flows SF1 and SF2](image)

Assume a mobile node establishes two service flows, called SF1 and SF2. This two service flows can belong to one interface or two different interfaces. The SF1 is peer-to-peer voice over IP traffic with its peers that mobile node’s port number is 49724 and the peer’s port is 56512. The SF2 is HTTP traffic with its peer that the peer’s port is 80.

When mobility access gateway receives the data packet of the mobile node’s service flow, it will send the Proxy Binding Update message to the local mobility anchor with the service flow identifier option and assigned downlink GRE key for this service flow.

0 The service flow identifier option for SF1 included in the Proxy Binding Update message is set as follows:

```
Service Flow Identifier field is SFID1=1 and PRO field is 0;
```

0 The service flow description option included in the service flow identifier option is set as follows: Type field is set to 0,
Source Port Range field is set to 49724, and Destination Port Range field is set to 56512.

0 The service flow identifier option for SF2 included in the Proxy Binding Update message is set as follows:

Service Flow Identifier field is SFID2=2 and PRO field is 0;

The service flow description option included in the service flow identifier option is set as follows: Type field is set to 0, and Destination Port Range field is set to 80.

If the service flow proxy binding update is accepted, the local mobility anchor will return a Proxy Binding Acknowledge message with service flow identifier option and the assigned uplink GRE key, and the Status field is set to 0 (success).

If the mobile access gateway doesn’t receive the data packet of the peer-to-peer voice over IP traffic from the mobile node for a long time, it will send the Proxy Binding Update message to the local mobility anchor again to delete this service flow binding.

0 The service flow identifier option included in the Proxy Binding Update message is set as follows: Service Flow Identifier field is set to 1, and PRO field is set to 2.
5. Mobility Access Gateway Operation

5.1. Binding Update List extensions

Service flow binding is conceptually stored in the binding update list entry of the mobile access gateway. To better implement the service flow based control, the original BULE should be extended to include the following parameters:

- SFID (service flow identifier): A service flow identifier for the service flow of the mobile node MUST be unique within the LMA.
- Packet filter attributes of the service flow that contained in the service flow description option.

5.2. Service Flow Proxy Binding Update Operation

When a service flow of the mobile node is started or terminated, the mobile access gateway will analyze the received data packets, generate the unique service flow identifier, and trigger the service flow binding update mechanism. It then sends the Proxy Binding Update message containing a service flow identifier and the assigned downlink GRE key for this binding to the local mobility anchor. The service flow identifier option MUST indicate valid Service Flow Identifier, PRO, Service Flow Description option fields.

When the mobile access gateway receives the proxy binding acknowledge containing the service flow identifier option from the local mobility anchor, the Status field of the service flow identifier indicates the status of the service flow binding on the local mobility anchor. If it is set to 0 to 127, it means that this service flow binding operation is accepted by the local mobility anchor, and the local mobility anchor will return the uplink GRE key for this service flow binding in the Proxy Binding Acknowledge message.

5.3. Data Forwarding Rules

As the service flow binding operation is succeed, the mobile access gateway and local mobility anchor sets up the bi-directional tunnel, and assigns downlink and uplink GRE Key for this service flow binding.

When the mobile access gateway receives a data packet from the mobile node, it MUST check that a service flow binding for the service flow that the data packet belongs to is created or not. If the bi-directional tunnel is set up, the mobile access gateway will
encapsulate the data packet with the uplink GRE key, and then forward it to the mobile node’s local mobility anchor.

When the mobile access gateway receives a data packet from the bidirectional tunnel established with the local mobility anchor, it will decapsulate the data packet by removing the outer header, and attains the destination address of the inner packet. Then the mobile access gateway will forward it to the mobile node on the interface where the destination network prefix is hosted.
6. Local Mobility Anchor Operation

6.1. Binding Cache extensions

Service flow binding is conceptually stored in the binding cache entry of the local mobility anchor. To better implement the service flow based control, the original BCE should be extended to include the following parameters:

- **SFID (service flow identifier):** A service flow identifier for the service flow of the mobile node MUST be unique within the LMA.
- **Packet filter attributes of the service flow that contained in the service flow description option.**

6.2. Service Flow Proxy Binding Acknowledge Operation

When the local mobility anchor receives the Proxy Binding Update message which includes the service flow identifier option, it first performs the operation described in section 5.3.1 of RFC 5213. If the proxy binding update is accepted, the local mobility anchor then checks the service flow identifier option.

If the PRO field in the service flow identifier option is set to 0 which indicates to add a new service flow binding, the local mobility anchor first checks the service flow identifier field that it MUST a value that does not already exist. Then the local mobility anchor checks the service flow description option following the service flow identifier option. If all of the checks above indicated a valid option, the local mobility anchor will return a Proxy Binding Acknowledge message with the Status field set to 0 and the uplink GRE key, and then add the service flow binding to its binding cache.

If the PRO field in the service flow identifier option indicates to modify or delete an existent service flow binding, the local mobility anchor first checks the service flow identifier field that it needs to contain a value that already exists. Then the local mobility anchor will return a Proxy Binding Acknowledge message with the uplink GRE key and modify or delete the corresponding service flow binding in its binding cache.

6.3. Data Forwarding Considerations

When the local mobility anchor receives a data packet from a correspondent node with the destination address matching a mobile...
node’s home network prefix field, with the source address matching the destination address field, and other attributes matching of the corresponding fields in the binding cache entry, it MUST encapsulate it with the downlink GRE key of this service flow binding, and forward it to the mobile access gateway through the bi-directional tunnel.

When the local mobility anchor receives a data packet from the bi-directional tunnel with the mobile access gateway, it MUST decapsulate the data packet by removing the outer header. Then it will forward the data packet to the destination address of the correspondent node in the inner header.
7. Security Considerations

Since the service flow identifier option is part of the mobility option in the proxy binding update and acknowledge message, it uses the same security as the proxy binding update operation in RFC 5213.
8. IANA Considerations

This specification defines two new mobility options as in section 2, the Service Flow Identifier Option and the Service Flow Description Option.
9. References

9.1. Normative References


9.2. Informative References


Author’s Addresses

Min Hui
China Mobile
53A, Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: huimin.cmcc@gmail.com

Gang Chen
China Mobile
53A, Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: chengang@chinamobile.com

Hui Deng
China Mobile
53A, Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: denghui02@gmail.com