NETLMM WG
Internet-Draft
Intended status: Standards Track
Expires: October 10, 2007

S. Gundavelli
K. Leung
Cisco
V. Devarapalli
Azaire Networks
K. Chowdhury
Starent Networks
B. Patil
Nokia Siemens Networks
April 08, 2007

Proxy Mobile IPv6
draft-ietf-netlmm-proxymip6-00.txt

Status of this Memo

Copyright Notice

Abstract

Host based IPv6 mobility is specified in Mobile IPv6 base specification [RFC3775]. In that model, the mobile node is

responsible for doing the signaling to its home agent to enable session continuity as it moves between subnets. The design principle in the case of host-based mobility relies on the mobile node being in control of the mobility management. Network based mobility allows IP session continuity for a mobile node without its involvement in mobility management. This specification describes a protocol solution for network based mobility management that relies on Mobile IPv6 signaling and reuse of home agent functionality. A proxy mobility agent in the network which manages the mobility for a mobile node is the reason for referring to this protocol as Proxy Mobile IPv6.

Table of Contents

1. Introduction

Mobile IPv6 [RFC-3775] is the enabler for IPv6 mobility. It requires Mobile IPv6 client functionality in the IPv6 stack of a mobile node. Signaling between the MN and HA enables the creation and maintenance of a binding between the MNs home address and care-of-address. Mobile IPv6 has been designed to be an integral part of the IPv6 stack in a host. However there exist IPv6 stacks today that do not have Mobile IPv6 functionality and there would likely be IPv6 stacks without MIPv6 functionality in the future as well. It is desirable to support IP mobility for all hosts irrespective of the presence or absence of mobile IPv6 functionality in the IPv6 stack.

It is possible to support mobility for IPv6 nodes by extending Mobile IPv6 [RFC-3775] signaling and reusing the home agent via a proxy mobility agent in the network. This approach to supporting mobility does not require the mobile node to be involved in the signaling required for mobility management. The proxy agent in the network performs the signaling and does the mobility management on behalf of the mobile node. Because of the use and extension of Mobile IPv6 signaling and home agent functionality, it is referred to as Proxy Mobile IPv6 (PMIP6) in the context of this document.

Network deployments which are designed to support mobility would be agnostic to the capability in the IPv6 stack of the nodes which it serves. IP mobility for nodes which have mobile IP client functionality in the IPv6 stack as well as those hosts which do not, would be supported by enabling PMIP6 protocol functionality in the network. The advantages of developing a network based mobility protocol based on Mobile IPv6 are:

- Reuse of home agent functionality and the messages/format used in mobility signaling. Mobile IPv6 is a mature protocol with several implementations that have been through interoperability testing.

- A common home agent would serve as the mobility agent for all types of IPv6 nodes.

- Addresses a real deployment need.

The problem statement and the need for a network based mobility protocol solution has been documented in [draft-ietf-netlmm-nohost-ps-05.txt]. PMIP6 is a solution that addresses these issues and requirements.

The IP Mobility protocols designed in the IETF so far involve the host in mobility management. There are some deployment scenarios where a network-based mobility management protocol is considered

appropriate. The advantages to using a network-based mobility protocol include avoiding tunneling overhead over the air and support for hosts that do not implement any mobility management protocol.

The document describes a network-based mobility management protocol based on Mobile IPv6. it is called Proxy Mobile IPv6 (PMIPv6). One of the most important design considerations behind PMIPv6 has been to re-use as much as possible from the existing mobility protocols.

There are many advantages to develop a protocol based on Mobile IPv6. Mobile IPv6 is a very mature mobility protocol for IPv6. There have been many implementations and inter-operability events where Mobile IPv6 has been tested. There also numerous specifications enhancing Mobile IPv6 that can be re-used. Further, the Proxy MIPv6 solution described in this document allows the same Home Agent to provide mobility to hosts that use Mobile IPv6 and hosts that do not use any mobility management protocol. Proxy Mobile IPv6 provides solution to a real deployment problem.

The specific details related to enabling IPv4 home address mobility for the mobile node and the details related to supporting IPv4 transport network are covered in the companion document.

2. Conventions & Terminology

2.1. Conventions used in this document

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in this document are to be interpreted as described in RFC 2119.

2.2. Terminology

All the general mobility related terms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC-3775].

This document adopts the terms, Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG) from the NETLMM Goals document [draft-ietf-netlmm-nohost-req-05.txt]. It further provides the following context specific explanation to these terms, specific to this solution document.

Local Mobility Anchor (LMA)

Local Mobility Anchor is the home agent for the mobile node in the Proxy Mobile IPv6 domain. It is the topological anchor point for the mobile node's home prefix and is the entity that manages the mobile node's reachability state. It is important to understand that the LMA has the functional capabilities of a home agent as defined in Mobile IPv6 base specification [RFC-3775] and with the additional required capabilities for supporting Proxy Mobile IPv6 as defined in this specification.

Proxy Mobile Agent (PMA)

Proxy mobility agent is a function that manages the mobility related signaling for a mobile node that is attached to its access link. It is responsible for tracking the mobile node's attachment to the link and for signaling the mobile node's local mobility anchor.

Mobile Access Gateway (MAG)

It is the entity where the Proxy Mobile Agent function resides.

Mobile Node (MN)

Through out this document, the term mobile node is used to refer to an IP node whose mobility is provided by the network. The mobile node may be operating in IPv6 mode, IPv4 mode or in IPv4/ IPv6 dual mode. The mobile node is not required to participate in any mobility related signaling for achieving mobility for an IP address that is obtained in that local domain. This document further uses explicit text when referring to a mobile node that is involved in mobility related signaling as per Mobile IPv6 specification [RFC-3775]. The mobile node's capability or its involvement in any mobility related signaling for obtaining mobility for an address that is obtained outside the current proxy mobile IPv6 domain, is not relevant in the context of this document and this definition of the Mobile Node shall survive.

Mobile Node's Home Address (MN-HoA)

MN-HoA is the home address of a mobile node in a Proxy Mobile IPv6 domain. It is an address obtained by the mobile node in that domain. The mobile node can continue to use this address as long as it is attached to the network that is in the scope of that Proxy Mobile IPv6 domain. When supporting IPv4 address mobility for a mobile node, the term, IPv4 MN-HoA is used to refer to the IPv4 address of the mobile node.

Proxy Care-of Address (Proxy-CoA)

Proxy-CoA is the address configured on the interface of the mobile access gateway and is the transport endpoint of the tunnel between the local mobility anchor and the mobile access gateway. The local mobility anchor views this address as the Care-of Address of the mobile node and registers it in the Binding Cache entry for that mobile node. When the transport network between the mobile access gateway and the local mobility anchor is an IPv4 network and if the care-of address that is registered at the local mobility anchor is an IPv4 address, the term, IPv4 Proxy-CoA is used.

LMA Address (LMAA)

The address that is configured on the interface of the local mobility anchor and is the transport endpoint of the tunnel between the local mobility anchor and the mobile access gateway. This is the address to where the mobile access gateway sends the Proxy Binding Update messages. When supporting IPv4 traversal, i.e. when the network between the local mobility anchor and the mobile access gateway is an IPv4 network, this address will be an IPv4 address and will be referred to as IPv4 LMAA.

Proxy Mobile IPv6 Domain (PMIPv6-Domain)

It is a localized mobility management domain. It is a portion of the access network where the mobility management of a mobile node is handled using Proxy Mobile IPv6 protocol as defined in this specification.

Mobile Node's Home Link

This is the link on which the mobile node obtained its initial address configuration after it moved into that Proxy Mobile IPv6 domain. This is the link that conceptually follows the mobile node. The network will ensure the mobile node always sees this link with respect to the layer-3 network configuration, on any access link that it attaches to in that proxy mobile IPv6 domain.

Mobile Node's Home Network Prefix (MN-HNP)

This is the on-link prefix that the mobile always sees in the Proxy Mobile IPv6 domain. The home network prefix is topologically anchored at the mobile's local mobility anchor. The mobile node configures its interface with an address from this prefix. When supporting IPv4 home address mobility, the term, IPv4 Home Network refers to the mobile node's IPv4 home prefix and the term, Home Network always refers to the IPv6 home network prefix.

Mobile Node Identifier (MN-Identifier)

The identity of the mobile node that is presented to the network as part of the access authentication. This is typically an identifier such as Mobile Node NAI [RFC-4283] any other type of identifier which may be specific to the access technology.

Proxy Binding Update (PBU)

A signaling message sent by the mobile access gateway to a mobile node's local mobility anchor for establishing a binding between the mobile node's MN-HoA and the Proxy-CoA.

Proxy Binding Acknowledgement (PBA)

A response message sent by a local mobility anchor in response to a Proxy Binding Update message that it received from a mobile access gateway.

3. Proxy Mobile IPv6 Protocol Overview

This specification describes a network-based mobility management protocol. It is called Proxy Mobile IPv6 (PMIPv6) and is based on Mobile IPv6 [RFC-3775]. This protocol is for providing network-based mobility management support to a mobile node, within a restricted and topologically localized portion of the network and with out requiring the participation of the mobile node in any mobility related signaling.

Every mobile node that roams in a Proxy Mobile IPv6 domain, would typically be identified by an identifier, such as MN-Identifier, and using that identifier the mobile node's policy profile can be obtained from the policy store. The policy profile typically contains the provisioned network-based mobility service characterstics and other related parameters such as the mobile node's home network prefix, permitted address configuration modes, roaming policy and other parameters that are essential for providing network based mobility service.

Once a mobile node enters its Proxy Mobile IPv6 domain and performs access authentication, the network will ensure the mobile node is always on its home network and further ensures the mobile node can always obtain its home address on the access link and using any of the address configuration procedures. In other words, there is home network prefix that is assigned for a mobile node and conceptually

that address always follows the mobile node, where ever it roams within that proxy mobile IPv6 domain. From the perspective of the mobile node, the entire Proxy Mobile IPv6 domain appears as its home link or a single link.

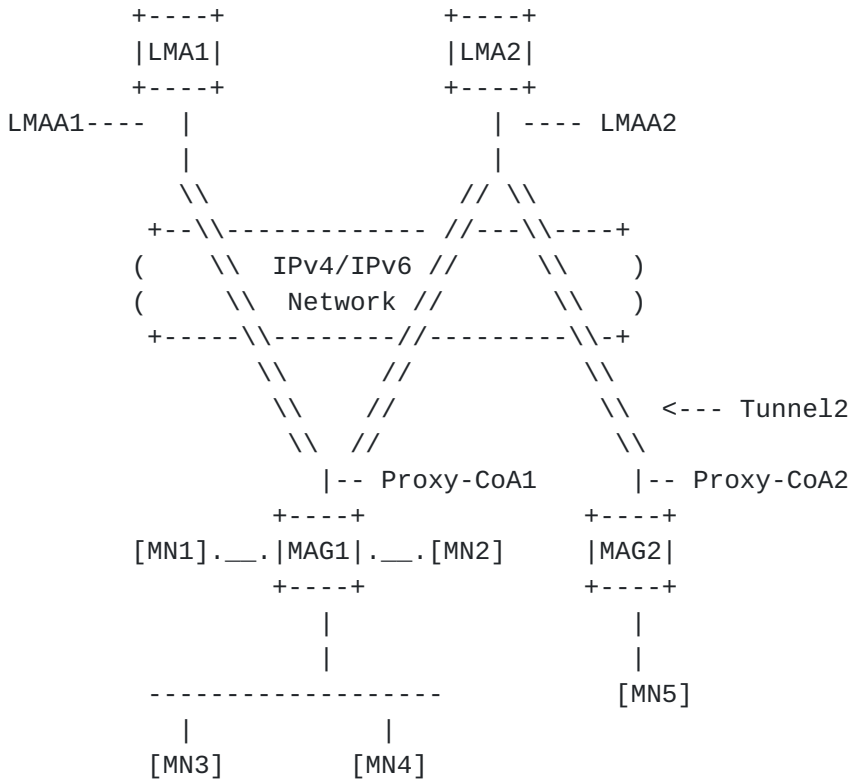


Figure 1: Proxy Mobile IPv6 Domain

The Proxy Mobile IPv6 scheme introduces a new function, the mobile access gateway. It is a function that is on the access link where the mobile is anchored and does the mobility related signaling on behalf of the mobile node. From the perspective of the local mobility anchor, the mobile access gateway is a special element in the network that is authorized to send Mobile IPv6 signaling messages on behalf of a mobile node.

When the mobile node attaches to an access link connected to the mobile access gateway, the mobile node presents its identity, MN-Identifier, as part of the access access authentication procedure. After a successful access authentication, the mobile access gateway obtains the mobile node's profile from the policy store, such as from

a AAA infrastructure. The mobile access gatway would have all the information for it to emulate the mobile node's home network on the access link. The mobile access gateway also starts sending periodic Router Advertisements to the mobile node advertising its home network prefix.

The mobile node on receiving these Router Advertisement messages on the access link will attempt to configure its interface either using statefull or stateless address configuration modes, based on modes that are permitted on that access link. At the end of a successful address configuration procedure, the mobile node would have obtained an address from its home network prefix. If the mobile node is IPv4 capable and if network offers IPv4 network mobility for the mobile node, the mobile node would have obtained an IPv4 address as well. The mobile node can be operating in IPv4-only mode, IPv6-only or in dual-mode and based on the services enabled for that mobile, the mobility is enabled only for those address types. Also, the network between the local mobility anchor and the mobile access gateway can be either IPv4, IPv6, IPv4 with NAT translation devices in the access network.

For updating the local mobility anchor about the current location of the mobile node, the mobile access gateway sends a Proxy Binding Update message to the mobile node's local mobility anchor. The message will have the mobile node's NAI identifier option and Home Network Prefix Option and/or IPv4 Home Address option. The source address of that message will be the address of the mobile access gateway on its egress interface. Upon accepting the Proxy Binding Update request, the local mobility anchor sends a Proxy Binding Acknowledgment message to the mobile access gateway. It also sets up a route to the mobile node's home network prefix over the tunnel and sends Proxy Binding Acknowledgment message to the mobile access gateway.

The mobile access gateway on receiving this Proxy Binding Acknowledgment message sets up a tunnel to the local mobility anchor and adds a default route over the tunnel to the local mobility anchor. All traffic from the mobile node gets routed to the mobile node's local mobility anchor over the tunnel.

At this point, the mobile node has a valid home address from its home network prefix, at the current point of attachment. The serving mobile access gateway and the local mobility anchor also have proper routing states for handling the traffic sent to and from the mobile node.

The local mobility anchor, being the topological anchor point for the mobile node's home network prefix, it receives any packet sent by any

corresponding node to the mobile node. Local mobility anchor forwards the received packet to the mobile access gateway through the tunnel. The mobile access gateway on other end of the tunnel, after receiving the packet removes the tunnel header and forwards the packet on the access link to the mobile node.

The mobile access gateway typically acts as a default router on the access link and any packet that the mobile node sends to any corresponding node is received by the mobile access gateway and it forwards the packet to the local mobility anchor through the tunnel. The local mobility anchor on the other end of the tunnel, after receiving the packet removes the tunnel header and routes the packet to the destination.

4. Proxy Mobile IPv6 Protocol Security

The signaling messages, Proxy Binding Update and Proxy Binding Acknowledgement, exchanged between the mobile access gateway and the local mobility anchor are protected using IPsec and using the established security association between them. The security association of the specific mobile node for which the signaling message is initiated is not required for protecting these messages.

ESP in transport mode with mandatory integrity protection is used for protecting the signaling messages. Confidentiality protection is not required.

IKEv2 is used to setup security associations between the mobile access gateway and the local mobility anchor to protect the Proxy Binding Update and Proxy Binding Acknowledgment messages. The mobile access gateway and the local mobility anchor can use any of the authentication mechanisms, as specified in IKEv2, for mutual authentication.

Mobile IPv6 specification requires the home agent to prevent a mobile node from creating security associations or creating binding cache entries for another mobile node's home address. In the protocol described in this document, the mobile node is not involved in creating security associations for protecting the signaling messages or sending binding updates. Therefore, this is not a concern. However, the local mobility anchor MUST allow only authorized mobile access gateways to create binding cache entries on behalf of the mobile nodes. The actual mechanism by which the local mobility anchor verifies if a specific mobile access gateway is authorized to send Proxy Binding Updates on behalf of a mobile node is outside the scope of this document. One possible way this could be achieved is

sending a query to the policy store such as by using AAA infrastrucure.

4.1. Peer Authorization Database Entries

The following describes PAD entries on the mobile access gateway and the local mobility anchor. The PAD entries are only example configurations. Note that the PAD is a logical concept and a particular mobile access gateway or a local mobility anchor implementation can implement the PAD in an implementation specific manner. The PAD state may also be distributed across various databases in a specific implementation.

```
mobile access gateway PAD:
  - IF remote_identity = lma_identity_1
       Then authenticate (shared secret/certificate/EAP)
       and authorize CHILD_SA for remote address lma_addres_1

local mobility anchor PAD:
  - IF remote_identity = mag_identity_1
       Then authenticate (shared secret/certificate/EAP)
       and authorize CHILD_SAs for remote address mag_address_1
```

The list of authentication mechanisms in the above examples is not exhaustive. There could be other credentials used for authentication stored in the PAD.

4.2. Security Policy Database Entries

The following describes the security policy entries on the mobile access gateway and the local mobility anchor required to protect the Proxy Mobile IPv6 signaling messages. The SPD entries are only example configurations. A particular mobile access gateway or a local mobility anchor implementation could configure different SPD entries as long as they provide the required security.

In the examples shown below, the identity of the mobile access gateway is assumed to be mag_1, the address of the mobile access gateway is assumed to be mag_address_1, and the address of the local mobility anchor is assumed to be lma_address_1.

```
mobile access gateway SPD-S:
  - IF local_address = mag_address_1 &
       remote_address = lma_address_1 &
       proto = MH & local_mh_type = BU & remote_mh_type = BAck
    Then use SA ESP transport mode
    Initiate using IDi = mag_1 to address lma_1

local mobility anchor SPD-S:
  - IF local_address = lma_address_1 &
       remote_address = mag_address_1 &
       proto = MH & local_mh_type = BAck & remote_mh_type = BU
    Then use SA ESP transport mode
```

5. Local Mobility Anchor Operation

For supporting the Proxy Mobile IPv6 scheme defined in this document, the Mobile IPv6 home agent entity, defined in Mobile IPv6 specification [RFC-3775], needs some protocol enhancements. The local mobility anchor is the functional entity with these capabilities for supporting Proxy Mobile IPv6. This section describes the operational details of the local mobility anchor.

The base Mobile IPv6 specification [RFC-3775], defines home agent and the mobile node as the two functional entities. The Proxy Mobile IPv6 scheme introduces a new entity, the mobile access gateway. This is the entity that will participate in the mobility related signaling. From the perspective of the local mobility anchor, the mobile access gateway is a special element in the network that has the privileges to send mobility related signaling messages on behalf of the mobile node. Typically, the local mobility anchor is provisioned with the list of mobile access gateways authorized to send proxy registrations.

When the local mobility anchor receives a Proxy Binding Update message from a mobile access gateway, the message is protected using the IPSec Security Association established between the local mobility anchor and the mobile access gateway. The local mobility anchor can distinguish between a Proxy Binding Update message received from a mobile access gateway from a Binding Update message received directly from a mobile node. This distinction is important for using the right security association for validating the Binding Update and this is achieved by relaxing the MUST requirement for having the Home Address Option presence in Destination Options header and by introducing a new flag in the Binding Update message. The local mobility anchor as a traditional IPSec peer can use the SPI in the IPSec header [RFC-4306] of the received packet for locating the

correct security association and for processing the Proxy Binding Update message in the context of the Proxy Mobile IPv6 scheme.

For protocol simplicity, the current specification supports the Per-MN-Prefix addressing model. In this addressing model, each mobile node is allocated an exclusively unique home network prefix and the prefix is not hosted on the home link. The local mobility anchor in this addressing model is just a topological anchor point and the prefix is physically hosted on the access link where the mobile node is attached. The local mobility anchor is not required to perform any proxy ND operations [RFC-2461] for defending the mobile node's home address, MN-HoA, on the home link. However, the local mobility anchor is required to manage the binding cache entry of the mobile node for managing the mobility session and also the routing state for creating a proper route path for traffic to/from the mobile node.

5.1. Extensions to Binding Cache Conceptual Data Structure

The local mobility anchor maintains a Binding Cache entry for each currently registered mobile node. Binding Cache is a conceptual data structure, described in Section 9.1 of [RFC3775]. For supporting this specification, the conceptual Binding Cache entry needs to be extended with the following new fields.

- A flag indicating whether or not this Binding Cache entry is created due to a proxy registration. This flag is enabled for Binding Cache entries that are proxy registrations and is turned off for all other entries that are direct registrations from the mobile node.

- A flag indicating if IPv6 HoA mobility is accepted. If this flag is set, the relevant IPv6 HoA fields in this data structure have to be set to the configured values. If this flag.

- The identifier of the mobile node, MN-Identifier. This MN-Identifier is obtained from the NAI Option present in the Proxy Binding Update request [RFC-4285].

- A flag indicating whether or not the Binding Cache entry has a home address that is on virtual interface. This flag is enabled, if the home prefix of the mobile is configured on a virtual interface. When the configured home prefix of a mobile is on a virtual interface, the home agent is not required to function as a Neighbor Discovery proxy for the mobile node.

- The IPv6 home network prefix of the mobile node.
- The IPv6 home network prefix length of the mobile node.
- The interface id of the tunnel between the local mobility anchor and the mobile access gateway used for sending and receiving the mobile node's traffic.
- Tentative binding cache entry with all the above fields. This entry is populated upon tentatively accepting a proxy binding update request for a mobile node whose direct registration still exists, i.e. the mobile has not deregistered and it received a proxy binding update request.

5.2. Bi-Directional Tunnel Management

The bi-directional tunnel between the local mobility anchor and the mobile access gateway is used for routing the traffic to and from the mobile node. The tunnel hides the topology and enables a mobile node to use an IP address that is topologically anchored at the local mobility anchor, from any attached access link in that proxy mobile IPv6 domain. The base Mobile IPv6 specification [RFC-3775], does use the tunneling scheme for routing traffic to and from the mobile that is using its home address. However, there are subtle differences in the way Proxy Mobile IPv6 uses the tunneling scheme.

As in Mobile IPv4 [RFC-3344], the tunnel between the local mobility anchor and the mobile access gateway is typically a shared tunnel and can be used for routing traffic streams for different mobile nodes attached to the same mobile access gateway. This specification extends that 1:1 relation between a tunnel and a binding cache entry to 1:m relation, reflecting the shared nature of the tunnel.

The tunnel is creating after accepting a Proxy Binding Update request for a mobile node from a mobile access gateway. The created tunnel may be shared with other mobile nodes attached to the same mobile access gateway and with the local mobility anchor having a binding cache entry for those mobile nodes. Some implementations may prefer to use static tunnels as supposed to creating and tearing them down on a need basis.

The one end point of the tunnel is the address configured on the interface of the local mobility anchor, LMAA. The other end point of the tunnel is the address configured on the interface of the mobile access gateway, Proxy-CoA. The tunnel encapsulation mode can be either IPv6/IPv6, IPv6/IPv4, IPv6/IPv4-UDP, IPv4/IPv6, IPv4/IPv4-UDP, based on the transport mode and the presence of NAT translation

devices on the path.

Implementations typically use a software timer for managing the tunnel lifetime and a counter for keeping a count of all the mobiles that are sharing the tunnel. The timer value will be set to the accepted binding life-time and will be updated after each periodic registrations for extending the lifetime. If the tunnel is shared for multiple mobile node's traffic, the tunnel lifetime will be set to the highest binding life time across all the binding life time that is granted for all the mobiles sharing that tunnel.

5.3. Routing Considerations

This section describes how the data traffic to/from the mobile node is handled at the local mobility anchor. The following entries explains the routing state that is created for the mobile node home network prefix.

```
IPv6 traffic for the Mobile Node's home address:
================================================
   MN-HoA::/64 via tunnel0, next-hop Proxy-CoA


tunnel0:
========
   Source:      LMAA
   Destination: Proxy-CoA
   Tunnel Transport: IPv6
   Tunnel Payload: IPv6
```

The local mobility anchor functions as a topological anchor point for the mobile node's home network prefix. When the local mobility anchor receives a data packet from a corresponding node, destined for the mobile node's home network prefix, the created routing state will enable the packets to be forwarded to the mobile node through the bi-directional tunnel established between itself and the serving mobile access gateway.

If the tunnel between the local mobility anchor and the mobile access gateway is an IPv6 tunnel, i.e. if the registered care-of address is the IPv6 Proxy-CoA, any IPv6 packets received from any corresponding node for the mobile node's home network prefix, MN-HNP, will be encapsulated in an IPv6 packet, IPv6/IPv6 mode, and will be carried as an IPv6 packet. And any IPv4 packets for the mobile node's IPv4-MN-HoA, will be encapsulated in an IPv6 packet, IPv4/IPv6 mode, and

will be carried as an IPv6 packet.

All the reverse tunneled packets that the local mobility anchor receives from the tunnel, after removing the packet encapsulation will get routed to the destination specified in the inner packet header. These routed packets will have the source address field set to the mobile node's home address.

5.4. Local Mobility Anchor Address Discovery

Dynamic Home Agent Address Discovery, as explained in Section 10.5 of [RFC-3775], allows a mobile node to discover all the home agents on its home link by sending an ICMP Home Agent Address Discovery Request message to the Mobile IPv6 Home-Agents anycast address, derived from its home network prefix.

The Proxy Mobile IPv6 model assumes that the mobile access gateway will be able to obtain the address of the local mobility anchor in one or more ways. This MAY be a configured entry in the mobile node's policy profile, or it MAY be obtained through mechanisms outside the scope of this document. It is important to note that there is little value in using DHAAD for discovering the local mobility anchor address dynamically. As a mobile moves from one mobile access gateway to the another, the serving mobile access gateway will not predictably be able to locate the serving local mobility anchor for that mobile that has its binding cache entry for the mobile node. However, if there is only one local mobility anchor configured to serve a mobile node, the mobile access gateway can use Dynamic Home Agent Address Discovery scheme for discovering the address of the local mobility anchor.

With the currently supported Per-MN-Prefix addressing model, every mobile node is assigned a unique home network prefix, the local mobility anchor is a topological anchor point for that prefix and with the prefix being hosted on the access link attached to the mobile access gateway. For the discovery scheme to work, the local mobility anchor MUST be able to receive the ICMP discovery packets sent to the anycast address derived from the mobile node's home network prefix.

5.5. Sequence Number and Time-Stamps for Message Ordering

Mobile IPv6 [RFC-3775] uses the Sequence Number field in registration messages as a way to ensure the correct packet ordering. The local

mobility anchor and the mobile node are required to manage this counter over the lifetime of a binding.

In Proxy Mobile IPv6, the Proxy Binding Update messages that the local mobility anchor receives on behalf of a specific mobile node may not be from the same mobile access gateway as the previously received message. It creates certain ambiguity and the local mobility anchor will not be predictably order the messages. This could lead to the local mobility anchor processing an older message from a mobile access gateway where the mobile node was previously attached, while ignoring the latest binding update message.

In the Proxy Mobile IPv6, the ordering of packets has to be established accross packets received from multiple senders. The sequence number scheme as specified in [RFC-3775] will not be sufficient. A global scale, such as a time stamp, can be used to ensure the correct ordering of the packets. This document proposes the use of a Time Stamp Option, specified in Section 8.4, in all Proxy Binding Update messages sent by mobile access gateways. By leveraging the NTP [RFC-1305] service, all the entities in Proxy Mobile IPv6 domain will be able to synchronize their respective clocks. Having a time stamp option in Proxy Binding Update messages will enable the local mobility anchor to predictably identify the latest message from a list of messages delivered in an out-of-order fashion.

The Proxy Mobile IP model, defined in this document requires the Binding Update messages sent by the mobile access gateway to have the time stamp option. The local mobility anchor processing a proxy registration MUST ignore the sequence number field and SHOULD use the value from the Time Stamp option to establish ordering of the received Binding Update messages. If the local mobility anchor receives a Binding Update message with an invalid Time Stamp Option, the Binding Update MUST be rejected and a Binding Acknowledgement MUST be returned in which the Status field is set to 148 (invalid time stamp option).

In the absence of Time Stamp option in the Proxy Binding Update, the entities can fall back to Sequence Number scheme for message ordering, as defined in RFC-3775. However, the specifics on how different mobile access gateways synchronize the sequence number is outside the scope of this document.

When using the Time Stamp Option, the local mobility anchor or the mobile access gateway MUST set the the timestamp field to a 64-bit value formatted as specified by the Network Time Protocol [RFC-1305]. The low-order 32 bits of the NTP format represent fractional seconds, and those bits which are not available from a time source SHOULD be

generated from a good source of randomness.

5.6. Route Optimizations Considerations

Mobile IPv6 route optimization, as defined in [RFC-3775], enables a mobile node to communicate with a corresponding node directly using its care-of address and further the Return Routability procedure enables the corresponding node to have reasonable trust that the mobile node owns both the home address and care-of address.

In the Proxy Mobile IPv6 model, the mobile is not involved in any mobility related signaling and also it does not operate in the dual-address mode. Hence, the return routability procedure as defined in RFC-3775 is not applicable for the proxy model. This document does not address the Route Optimization problem and leaves this work item for future enhancements.

5.7. Mobile Prefix Discovery Considerations

The ICMP Mobile Prefix Advertisement message, described in Section 6.8 and Section 11.4.3 of [RFC-3775], allows a home agent to send a Mobile Prefix Advertisement to the mobile node.

In Proxy Mobile IPv6 deployments, the mobile node's home network prefix is hosted on the access link shared between the mobile access gateway and the mobile node, but topologically anchored on the local mobility anchor. Since, there is no physical home-link for the mobile node's home network prefix on the local mobility anchor and as the mobile is always on the link where the prefix is hosted, any prefix change messages can just be advertised by the mobile access gateway on the access link and thus there is no applicability of this messaging for Proxy Mobile IPv6. This specification does not support Mobile Prefix Discovery.

5.8. Local Mobility Anchor Operational Summary

- For supporting this scheme, the local mobility anchor MUST satisfy all the requirements listed in Section 8.4 of Mobile IPv6 specification [RFC-3775] with the following considerations.

- For supporting the per-MN-Prefix addressing model as defined in this specification, the local mobility anchor service MUST NOT be tied to a specific interface. It SHOULD be able to accept Proxy Binding Update requests sent to any of the addresses configured on any of its interfaces.

- The requirement for a home agent to maintain a list of home agents for a mobile node's home link is not applicable for the local mobility anchor, when supporting Per-MN-Prefix addressing model as there is no link specific relation between the two.

- After receiving a Proxy Binding Update request from a mobile access gateway on behalf of mobile node, the local mobility anchor MUST process the request as defined in Section 10, of the base Mobile IPv6 specification [RFC-3775], with one exception that this request is a proxy request, the sender is not the mobile node and so the message has to be processed with the considerations explained in this section.

- The local mobility anchor MUST apply the required policy checks, as explained in Section 4.0 of this document to verify the sender is a a trusted mobile access gateway, authorized to send proxy binding updates requests on behalf of that mobile nodes, using its own identity. The local mobility anchor must check the local/ remote policy store to ensure the requesting node is authorized to send proxy binding update requests.

- Upon accepting a proxy binding update request from a mobile access gateway, the local mobility anchor must check if there exists a binding cache entry for that mobile node, identified using the MN-Identifier, that was created due to a direct registration from the mobile node. If there exists a binding cache entry with the proxy registration flag turned off, the local mobility anchor MUST NOT modify that binding state, instead it must create a tentative binding cache entry and update the tentative binding cache entry fields of that binding cache entry.

- Upon receiving a Binding Update request from a mobile node with lifetime value set to 0, from a tunnel between itself and a trusted mobile access gateway, the local mobility anchor upon accepting that de-registration message, MUST forward the Binding Acknowledgement message in the tunnel from where it received the Binding Update request. It must also replace the binding cache entry with the tentative binding cache entry and enable routing for the mobile node's home prefix through the proxy mobile IPv6 tunnel.

- The local mobility anchor MUST use the MN-Identifier present in the NAI option of the Proxy Binding Update request for identifying the mobile node.

- The local mobility anchor MUST ensure the prefix presented in the Home Network Prefix option of the received Proxy Binding Update request is owned by itself and further the mobile node identified

by MN-Identifier is authorized to use this prefix.

- The local mobility anchor MUST ignore the sequence number field in the Proxy Binding Updates requests, if the Time-Stamp Option is present in the message. It must also skip all the checks related to sequence number as suggested in the Mobile IPv6 specification [RFC-3775]. However, the received sequence number MUST be copied and returned in the Proxy Binding Acknowledgement sent to the mobile access gateway.

- Upon accepting this request, the local mobility anchor must create a Binding Cache entry with the home address from the Home Network Prefix Option in the Binding Update and must set up a tunnel to the proxy mobile agent serving the mobile node. This bi-directional tunnel between the local mobility anchor and the mobile access gateway is used for routing the mobile traffic.

- The local mobility anchors SHOULD drop all HoTI messages received for a home address that has corresponding Binding Cache entry with the proxy registration flag set.

- The local mobility anchor must handle the mobile node's data traffic as explained in the Routing Considerations section of this document.

6. Mobile Access Gateway Operation

The Proxy Mobile IPv6 scheme specified in this document, introduces a new functional entity, the Mobile Access Gateway (MAG). It is the entity that detects the mobile node's movements and initiates the signaling with the mobile node's local mobility anchor for updating the route to the mobile node's home address. In essence, the mobile access gateway performs mobility management on behalf of the mobile node.

From the perspective of the local mobility anchor, the mobile access gateway is a special element in the network that sends Mobile IPv6 signaling messages on behalf of a mobile node, but using its own identity. It is the entity that binds the mobile node's home address to an address on its own access interface.

The mobile access gateway has the following functional roles.

- It is responsible for detecting the mobile node's attachment or detachment on the connected access link and for initiating the mobility signaling to the mobile node's local mobility anchor.

- Emulation of the mobile node's home link on the access link.

- It is responsible for setting up the data path for enabling the mobile node to use its home address for communication from the access link.

This Proxy Mobile IPv6 scheme is independent of the underlying access technology or the link model. The interface between the mobile node and the mobile access gateway can be either:

- Point-to-Point Link

- Shared Link

This specification does not support split links.

6.1. Address Configuration Models

Currently, this specification only supports Per-MN-Prefix model In the Per-MN-Prefix model, there is a unique home network prefix assigned for each mobile node and that prefix is hosted on the access link. Conceptually, the prefix just follows the mobile node as it moves within the proxy mobile IPv6 domain. In this addressing model, based on the administrative policy, the mobile node can use either Stateless Address Autoconfiguration or Statefull Address Configuration using DHCP for obtaining the IPv6 address configuration for its interface on the access link. Further, the mobile node can also generate interface identifiers with privacy considerations, as specified in Privacy Extensions specification [RFC-3041] and as per CGA specification [RFC-3042]. For IPv4 home address configuration, the mobile node can obtain the address configuration using DHCP or optionally by using IPCP. In addition to this, Other address configuration mechanisms specific to the access link between the mobile node and the mobile access gateway may also be used by the mobile node.

The configured administrative policy for the mobile dictates the type of addressing model that is supported for a mobile on the access link. The mobile access gateway on the access router will control this by setting the relevant flags in the Router Advertisement that it sends on the access link.

6.2. Conceptual Data Structures

Every mobile access gateway maintains a Binding Update List for each currently attached mobile node. The Binding Update List is a conceptual data structure, described in Section 11.1 of Mobile IPv6 base specification [RFC-3775]. For supporting this specification, the conceptual Binding Update List data structure must be extended with the following new additional fields.

- The Identifier of the mobile node, MN-Identifier. The format of the MN-Identifier is specific to the access technology. This MN identifier is obtained as part of the Access Authentication procedure and is used for downloading the mobile node's profile from the policy store.
- The physical address or the MAC address of the mobile node's connected interface.
- The IPv6 home network prefix of the mobile node.
- The IPv6 home network prefix length of the mobile node.
- The link-local address of the mobile node on the link. This address MAY be learnt from the source address of the Router Solicitation message received from the mobile node.
- The tunnel identifier of the tunnel between the mobile access gateway and the local mobility anchor used for reverse tunneling the mobile node's traffic. On a given implementation, if a tunnel appears like a virtual interface, that applies the proper encapsulation on every packet that is routed through that interface, then the interface identifier is stored in the binding update list. entry.

6.3. Access Authentication

When a mobile node attaches to the access link connected to the mobile access gateway, the deployed access security protocols will ensure that only authorized mobile nodes will be able to access the link and further the mobile access gateway will be able to identify the mobile node by its MN-Identifier and optionally will be able to detect the mobile node's attachment or detachment to the link. The exact specifics on how this is achieved is outside the scope of this document. This document goes with the stated assumption of having an established trust between the mobile node and mobile access gateway on the access link before the protocol operation begins. The mobile

access gateway will be able to use the mobile node's MN-Identity and will be obtain its policy profile from the network policy store or from the local policy store.

6.4. Home Network Emulation

One of the key functions of the mobile access gateway is to emulate the mobile node's home network on the access link. It has to ensure, the mobile node believes it is connected to its home link or the link where it obtained its address configuration after it moved into that proxy mobile IPv6 domain. After the access authentication is complete, the mobile access gateway will have access to the mobile node's profile, obtained from querying a local/network policy store or provided to it as part of some context transfer procedure. After this point, the mobile access gateway will have enough information to emulate the mobile node's home link. It must send the Router Advertisement messages advertising the mobile node's home network prefix and other parameters.

If the access link connecting the mobile access gateway and the mobile node is a point-to-point link, the Router Advertisements advertising a specific home network prefix is received only by the respective mobile node and hence there is clearly a unique link for each mobile node that is attached to that mobile access gateway.

If the access link connecting the mobile access gateway and the mobile node is a shared-link, the mobile access gateway MUST ensure that each of the mobile node that is attached to that link receives Router Advertisements with its respective home network prefix as the on-link prefix. For this to happen, the mobile access gateway MUST unicast the Router Advertisement to the mobile node. The destination field of the link-layer header in the Router Advertisement MUST be the mobile's node's interface physical/MAC address and however, the destination field in the IPv6 header set to the all-nodes-multicast address.

6.5. Link-Local and Global Address Uniqueness

A mobile node in a proxy mobile IPv6 domain, as it moves from one access link to the other, will continue to detect its home network and hence the issue of link-local address uniqueness arises. The link-local that the mobile node attempts to use on the new link must be unique.

On a point-to-point link, such as in a PPP session, when the mobile node tries to establish a PPP session [RFC-1661] with the mobile

access gateway, the PPP goes through the Network layer Protocol phase and the IPv6 Control Protocol, IPCP6 [RFC-2472] gets triggered. Both the PPP peers negotiate a unique identifier using Interface-Identifier option in IPV6CP and the negotiated identifier is used for generating a unique link-local address on that link. Now, if the mobile node moves to a new access router, the PPP session gets torn down and new PPP session with the new mobile access gateway will be established and the mobile obtains a new link-local address. Now, even if the mobile is DNAv6 capable, as specified in the DNAv6 specification [draft-ietf-dna-protocol-03], the mobile node always configures a new link-local address when ever it moves to a new link.

However, if the link between the mobile node and the mobile access gateway is a shared link and if a DNAv6 capable mobile node moves from one access link to the other, the mobile node may not detect a link change due to the optimizations from DNAv6 and hence there is a possibility of the link-local address collision on the connected access link, One of the work around for this issue to the set following flag on the mobile node, DNASameLinkDADFlag to TRUE and that will force the mobile node to redo DAD operation even when DNAv6 detects no link change.

The global address or the MN-HoA uniqueness is assured as the uniqueness is established by the local mobility anchor before accepting a proxy binding update for a mobile node. This is further assured with the currently supported per-mn-prefix model, as there are two mobile nodes that share the same home network prefix. Further, if the address configuration is based on statefull address configuration using DHCP, the DHCP server will ensure the uniqueness.

6.6. Tunnel Management

In the traditional Mobile IPv6 model, there is a separate tunnel from the local mobility anchor to every mobile node that has a binding cache entry. The one end-point of these tunnels is the respective mobile node's care-of address and that is unique to that mobile node. In the case of Proxy Mobile IPv6, the care-of address or the tunnel end-point is the address of the mobile access gateway and there could be multiple mobile nodes attached to the same mobile access gateway and hence the tunnel is a shared tunnel serving multiple mobile nodes. This is identical to the Mobile IPv4 model [RFC-3344], where a tunnel between the foreign agent and the home agent is shared by many visiting mobile nodes and hence the tunnel management needs to be on a global basis and not be dependent on a specific mobile node's binding.

The life of the Proxy Mobile IPv6 tunnel should not be based on a

single binding cache entry. The tunnel may get created as part of creating a mobility state for a mobile node and later the same tunnel may be associated with other mobile nodes. So, the tearing down logic of the tunnel must be based on the number of visitors over that tunnel. Implementations are free to pre-establish tunnels between every local mobility anchor and every mobile access gateway in a proxy mobile IPv6 domain and with out having to create and destroy the tunnels on a need basis.

6.7. Routing Considerations

This section describes how the data traffic to/from the mobile node is handled at the mobile access gateway. The following entries explains the routing state for the mobile node on the mobile access gateway.

Mobile Node's IPv6 traffic:
==========
For all traffic from the source address MN-HoA to destination 0::/0 route via tunnel0, next-hop LMAA.

MN-HoA::/64 is reachable via the directly connected interface.

tunnel0:
========
   Source: Proxy-CoA
   Destination: LMAA
   Tunnel Payload: IPv6
   Tunnel Transport: IPv6

When the mobile access gateway receives any packets from the mobile node to any destination, the packet will be forwarded to the local mobility anchor through the bi-directional tunnel established between itself and the mobile's local mobility anchor. However, the packets that are sent with link-local source address are not forwarded.

If the tunnel between the mobile access gateway and local mobility anchor is an IPv6 tunnel i.e. if the registered care-of address is an IPv6 Proxy-CoA, any IPv6 packet from the mobile node with the source MN-HoA, will be encapsulated in an IPv6 packet, IPv6/IPv6 mode and will be carried as an IPv6 packet. And any IPv4 packet from the mobile node with the source IPv4 Mobile-HoA, will be encapsulated in

an IPv6 packet, IPv4/IPv6 mode, and will be carried as an IPv6 packet.

All the packets that the mobile access gateway receives from the tunnel, after removing the tunnel encapsulation, will forward it to the mobile node on the connected interface.

6.8. Interaction with DHCP Relay Agent

If Statefull Address Configuration using DHCP is supported on the link on which the mobile node is attached, the DHCP relay agent [RFC-3315] needs to be configured on the access router. When the mobile node sends a DHCPv6 Request message, the relay agent function on the access router must set the link-address field in the DHCPv6 message to the mobile node's home network prefix, so as to provide a prefix hint to the DHCP Server. On a point-to-point link, this is just a normal DHCP relay agent configuration. However, on the shared links supporting multiple mobile nodes with different home prefixes, there is some interaction required between the relay agent and the mobile access gateway, for setting the link-address field to the requesting mobile node's home network prefix.

6.9. Mobile Node Detachment Detection and Resource Cleanup

Before sending a Proxy Binding Update message to the local mobility anchor for extending the lifetime of a currently existing binding of a mobile node, the mobile access gateway MUST make sure the mobile node is still attached to the connected link by using some reliable method. If the mobile access gateway cannot predictably detect the presence of the mobile node on the connected link, it MUST NOT attempt to extend the registration lifetime of the mobile node. Further, in such scenario, the mobile access gateway MUST terminate the binding of the mobile node by sending a Proxy Binding Update message to the mobile node's local mobility anchor with lifetime value set to 0. It MUST also remove any local state such as binding update list entry that was created for that mobile node.

The specific detection mechanism of the loss of a visiting mobile node on the connected link is specific to the access link between the mobile node and the mobile access gateway and is outside the scope of this document. Typically, there are various link-layer specific events specific to each access technology that the mobile access gateway can depend on for detecting the node loss. In general, the mobile access gateway can depend on one or more of the following methods for the detection presence of the mobile node on the

connected link:

- Link-layer event specific to the access technology
- PPP Session termination event on point-to-point link types
- IPv6 Neighbor Unreachability Detection event from IPv6 stack
- Notification event from the local mobility anchor
- Absence of data traffic from the mobile node on the link for a certain duration of time

6.10. Coexistence with Mobile Nodes using Host-based Mobility

In some operating environments, network operators may want to provision the access link attached to the mobile access gateway to offer network-based mobility service only to some nodes and enable normal IP access support for some other nodes on that link. This specification supports access links with such mixture of nodes. The network has the control on when to enable the mobile node with the network mobility service.

Upon obtaining the mobile node's profile after a successful access authentication and after a policy consideration, the mobile access gateway MUST determine if the network based mobility service should be offered to that mobile node. If the mobile node is entitled for such service, then the network should ensure the mobile node believes it is on its home link, as explained in various sections of this document.

If the mobile node is not entitled for the network based mobility service, as determined from the policy, the mobile access gateway MUST ensure the mobile node can obtain an IPv6 address using normal IPv6 address configuration mechanisms. The obtained address should be from a local visitor network prefix. In other words the mobile node should be able to operate as a traditional mobile node roaming in a visitor network and with the ability to obtain an address from the local visitor network prefix hosted on that link. This essentially ensures, the proxy mobile IPv6 protocol will not impact the behavior of a mobile node that is using host-based mobility, as per [RFC-3775].

If the stateless address configuration mode is supported on that link, the prefix information option in the router advertisements should contain local visitor network prefix. If statefull address configuration mode is enforced on the link and if DHCP is in used,

the mobile node should be able to obtain the IPv6 care-of address from the local visitor network prefix.

If the link between the mobile access gateway and the mobile node is a shared link, the Router Advertisement has to unicasted to the mobile node with the destination address in the layer-2 header set to the mobile's MAC address and the destination address in the IPv6 header set to the all-nodes multicast address.

6.11. Mobile Access Gateway Operation Summary

- After detecting a new mobile node on its access link and after the successful access authentication and authorization of the mobile node, the mobile access gateway MUST be able to able to access the mobile node's profile. This may be downloaded from the local/ network policy store using MN-Identity or may be obtained as part of a context transfer procedure. The mobile node's profile at the minimum MUST have the mobile node's local mobility anchor address and the MN-Identity. Optionally, it may have the mobile node's home network prefix and other configuration parameters.

- The mobile access gateway MAY use one or more ways to detect the attachment of a mobile node on to the link. The techniques can be specific to the access technology or can be other generic events as mentioned in the above sections.

- If the network determines that the mobile node will not be offered the network-based mobility service, the mobile access gateway MUST ensure that the Router Advertisements it sends will not contain the mobile node's home prefix, but will be the hosted on-link prefix. Also, if the mobile node attempts to obtain an IPv6 address, the mobile access gateway or the DHCP relay agent on the link MUST ensure that the prefix hint that gets added to the DHCP message will be of the local hosted prefix.

- `The mobile access gateway on receiving a Router Solicitation message from a mobile node MUST send a Router Advertisement message containing the mobile node's home network prefix.

- The mobile access gateway MUST send the periodic Router Advertisement messages, as per the ND specification [RFC-2461], advertising the mobile node's home network prefix on the access link.

- If the link between the mobile node and the mobile access gateway is a shared-link, then the Router Advertisement MUST be unicasted to the mobile node by setting the destination address in the link-

layer header to the mobile node's MAC address and with the destination address in the IPv6 header set to the all-nodes multicast address.

- If the mobile node uses DHCP for address configuration, the mobile access gateway or specifically the DHCP relay agent on the link MUST ensure the DHCPv4/v6 packets are properly tagged with the sending mobile node's MN-HoA, as the prefix hint.

- The Proxy Binding Update message that the mobile access gateway sends to the local mobility anchor, MUST have the configured IPv6 address of the egress interface. The Proxy Binding Update message MUST have the NAI option identifying the mobile node, home network prefix option and optionally the time stamp option. If the home network prefix option is set to value 0, the local mobility anchor will assign the home network prefix and will return them in the Proxy Binding Acknowledgment. This message MUST be protected by using IPSec security association created between the mobile access gateway and local mobility anchor.

- After receiving a Proxy Binding Acknowledgment with the status code indicating the acceptance of the Binding Update, the mobile access gateway MUST setup a tunnel to the mobile node's local mobility anchor, as explained in the above sections, if there is exists no tunnel. The mobile access gateway MUST also add a default route over the tunnel for all the traffic from the mobile node.

- If the local mobility anchor denies the Proxy Binding Update request, the mobile access gateways MUST NOT advertise the mobile node's home prefix on the access link and there by denying mobility service to the mobile node.

- Before attempting to extend binding lifetime of a mobile node, the mobile access gateway MUST make sure the mobile node is still attached to the connected link by using some reliable method. If the mobile access gateway cannot predictably detect the presence of the mobile node on the connected link, it MUST NOT attempt to extend the registration lifetime of the mobile node. Also, it MUST terminate the binding of the mobile node by sending a Proxy Binding Update message to the mobile node's local mobility anchor with lifetime value set to 0.

- At any point, if the mobile access gateway detects that the mobile node has roamed away from its access link, it MUST send a Proxy Binding Update to the local mobility anchor with the lifetime value set to 0 and it must also remove the default route over the tunnel for that mobile and also remove the Binding Update list

entry and any other local state created for that mobile node.

7. Mobile Node Operation

The Network-based mobility scheme defined in this document, allows a mobile node to obtain IP mobility within the proxy mobile IPv6 domain, with out requiring the mobile node to involve in any mobility management.

When a mobile node enters a proxy mobile IPv6 domain and attached to an access link, the network identifies the mobile node as part of the access authentication and establishes an identity for the mobile node. This identity has a binding to a cryptographic state and potentially associating the mobile node's link-layer address of the attached interface. The specifics on how this is achieved is beyond the scope of this document and is very much specific to the access technology and depends on the applied security protocols in place. For all practical purposes, this document assumes that the mobile node's access to the network is secure.

Once the mobile node enters a Proxy Mobile IPv6 domain and attaches to an access network, the network identifies the mobile as part of the access authentication procedure and ensures the mobile using any of the address configuration mechanisms permitted by the network for that mobile, will be able to obtain an address and move anywhere in that managed domain. From the perspective of the mobile, the entire Proxy Mobile IPv6 domain appears as a single link, the network ensures the mobile believes it is always on the same link.

The mobile node can be operating in an IPv4-only mode, IPv6-only mode or in dual IPv4/IPv6 mode. Typically, the configured policy in the network determines the type of home address(es) i.e. MN-HoA, IPv4 MN-HoA or both, that the network mobility is supported for. If the configured policy for a mobile node is for IPv6-only home address mobility, the mobile node will be able to obtain its MN-HoA, any where in that proxy mobile IPv6 domain and if policy allows only IPv4-only home address mobility, the mobile node will be able to obtain its IPv4 MN-HoA, any where in that domain. Similarly, if the policy permits both the IPv4 and IPv6 home address mobility, the mobile node will be able to obtain its MN-HoA and IPv4 MN-HoA and move anywhere in the network. However, if the mobile node is configured for IPv6-only mobility and if the mobile node attempts to obtain an IPv4 address configuration via DHCP mechanism, the obtained address configuration will not have any mobility properties, i.e. the

obtained address will be from a local prefix and not from a prefix that is topologically anchored at the local mobility anchor and hence the mobile will loose that address as it moves to a different link. The specifics on how this is achieved is the operational logic of the mobile access gateway on the access link.

7.1. Booting up in a Proxy Mobile IPv6 Domain

When a mobile node moves into a proxy mobile IPv6 domain and attaches to an access link, the mobile node will present its identity, MN-Identity, to the network as part of the access authentication procedure. Once the authentication procedure is complete and the mobile node is authorized to access the network, the network or specifically the mobile access gateway on the access link will have the mobile node's profile and so it would know the mobile node's home network prefix and the permitted address configuration modes. The mobile node's home network prefix may also be dynamically assigned by the mobile node's local mobility anchor and the same may be learnt by the mobile access gateway.

If the mobile node is IPv6 enabled, on attaching to the link and after access authentication, the mobile node typically would send a Router Solicitation message. The mobile access gateway on the attached link will respond to the Router Solicitation message with a Router Advertisement. The Router Advertisement will have the mobile node's home network prefix, default-router address and other address configuration parameters. The address configuration parameters such as Managed Address Configuration, Statefull Configuration flag values will typically be consistent through out that domain for that mobile node.

If the Router Advertisement has the Managed Address Configuration flag set, the mobile node, as it would normally do, will send a DHCPv6 Request and the mobile access gateway on that access link will ensure, the mobile node node gets the MN-HoA as a lease from the DHCP server.

If the Router Advertisement does not have the Managed Address Configuration flag set and if the mobile node is allowed to use an autoconfigured address, the mobile node will generate an interface identifier, as per the Autoconf specification [RFC-2462] or using privacy extensions as specified in Privacy Extensions specification [RFC-3041].

If the mobile node is IPv4 enabled or IPv4-only enabled, the mobile node after the access authentication, will be able to obtain the IPv4 address configuration for the connected interface by using DHCPv4.

Once the address configuration is complete, the mobile node will have the MN-HoA, IPv4 MN-HoA or both, that it can continue to use as long as it is with in the scope of that proxy mobile IPv6 domain.

7.2. Roaming in the Proxy Mobile IPv6 Network

After booting in the Proxy Mobile IPv6 domain and obtaining the address configuration, the mobile node as it roams in the network between access links, will always detect its home network prefix on the link, as long as the attached access network is in the scope of that proxy mobile IPv6 domain. The mobile node can continue to use its IPv4/IPv6 MN-HoA for sending and receiving packets. If the mobile node uses DHCP for address configuration, it will always be able to obtain its MN-HoA using DHCP. However, the mobile node will always detect a new default-router on each connected link, but still advertising the mobile node's home prefix as the on-link prefix and with the other configuration parameters consistent with the link properties as before.

7.3. IPv6 Host Protocol Parameters

This specification assumes the mobile node to be a normal IPv6 node, with its protocol operation consistent with the base IPv6 specification [RFC-2460]. All aspects of Neighbor Discovery Protocol, including Router Discovery, Neighbor Discovery, Address Configuration procedures will just remain consistent with the base IPv6 Neighbor Discovery Specification [RFC-2461]. However, this specification recommends that the following IPv6 operating parameters on the mobile node be adjusted to the below recommended values for protocol efficiency and for achieving faster hand-offs.

Lower Default-Router List Cache Time-out:

As per the base IPv6 specification [RFC-2460], each IPv6 host will maintain certain host data structures including a Default-Router list. This is the list of on-link routers that have sent Router Advertisement messages and are eligible to be default routers on that link. The Router Lifetime field in the received Router Advertisement defines the life of this entry.

In the Proxy Mobile IPv6 scenario, when the mobile node moves from one link to another, the received Router Advertisement messages advertising the mobile's home network prefix will be from a different

link-local address and thus making the mobile node believe that there is a new default-router on the link. It is important that the mobile node uses the newly learnt default-router as supposed to the previously learnt default-router. The mobile node must update its default-router list with the new default router entry and must age out the previously learnt default router entry from its cache, just as specified in Section 6.3.5 of the base IPv6 ND specification [RFC-2461]. This action is critical for minimizing packet losses during a hand off switch

On detecting a reachability problem, the mobile node will certainly detect the neighbor or the default-router unreachability by performing a Neighbor Unreachability Detection procedure, but it is important that the mobile node times out the previous default router entry at the earliest. If a given IPv6 host implementation has the provision to adjust these flush timers, still conforming to the base IPv6 ND specification, it is desirable to keep the flush-timers to suit the above consideration.

However, if the mobile access gateway has the ability to with draw the previous default-router entry, by multicasting a Router Advertisement using the link-local address that of the previous mobility proxy agent and with the Router Lifetime field set to value 0, then it is possible to force the flush out of the Previous Default-Router entry from the mobile node's cache. This certainly requires some context-transfer mechanisms in place for notifying the link-local address of the default-router on the previous link to the mobile access gateway on the new link.

There are other solutions possible for this problem, including the assignment of a unique link-local address for all the access routers in the Proxy Mobile IPv6 Network. In either case, this is an implementation choice and has no bearing on the protocol interoperability. Implementations are free to adopt the best approach that suits their target deployments.

8. Message Formats

This section defines extensions to the Mobile IPv6 [RFC-3775] protocol messages.

8.1. Proxy Binding Update

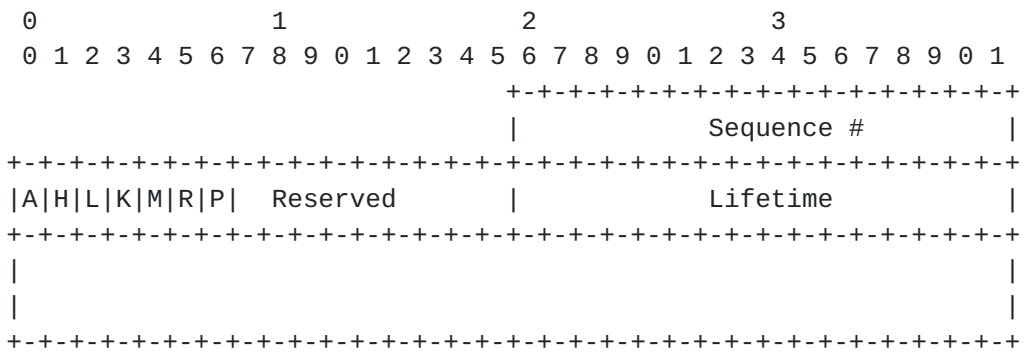


Figure 6: Proxy Binding Update Message

A Binding Update message that is sent by mobile access gateway is referred to as the Proxy Binding Update message.

Proxy Registration Flag (P)

The Proxy Registration Flag is set to indicate to the local mobility anchor that the Binding Update is from a mobile access gateway acting as a proxy mobility agent. The flag MUST be set to the value of 1 for proxy registrations and MUST be set to 0 for direct registration send my a mobile node using host-base mobility.

For descriptions of other fields present in this message, refer to the section 6.1.7 of Mobile IPv6 specification [RFC3775].

8.2. Proxy Binding Acknowledgment

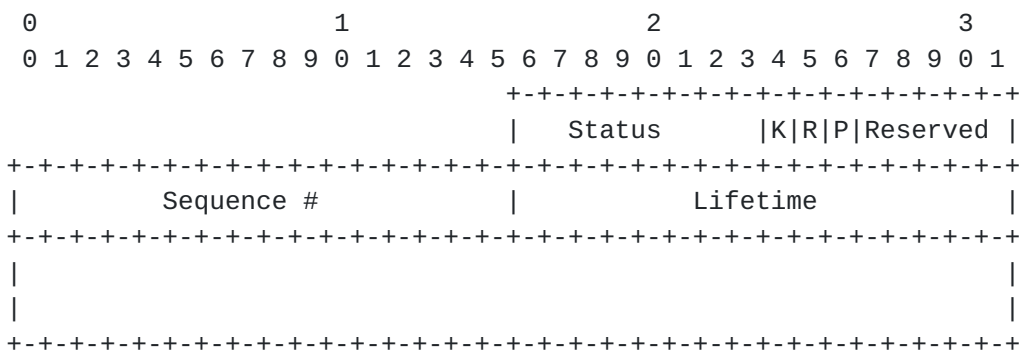


Figure 7: Proxy Binding Acknowledgment Message

Proxy Registration Flag (P)

A new flag (P) is included in the Binding Acknowledgement message to indicate that the local mobility anchor Agent that processed the corresponding Binding Update supports Proxy Registrations. The flag is set only if the corresponding Proxy Binding Update had the Proxy Registration Flag (P) set to 1. The rest of the Binding Acknowledgement format remains the same, as defined in [RFC-3775].

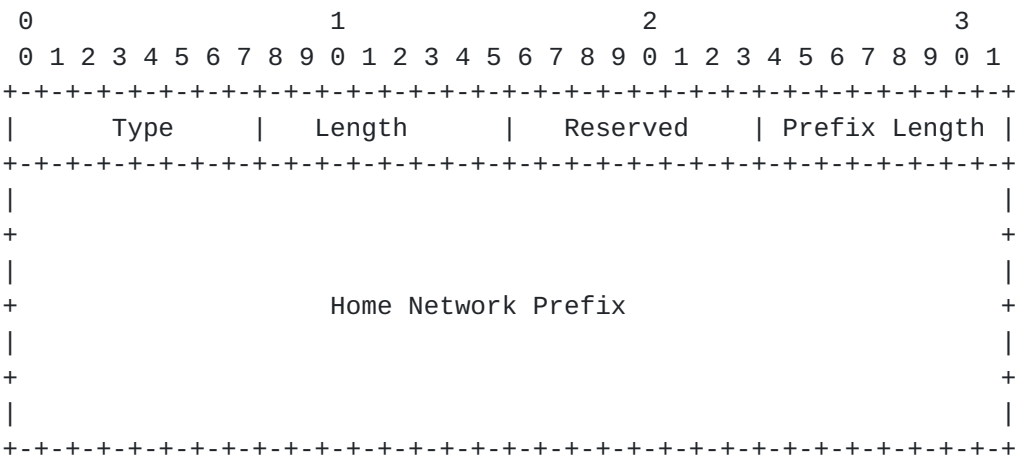
For descriptions of other fields present in this message, refer to the Mobile IPv6 base specificatoin [RFC-3775].

A Binding Acknowledgment message that is sent by the mobile access gateway is also referred to as "Proxy Binding Acknowledgement".

8.3. Home Network Prefix Option

A new option, Home Network Prefix Option is defined for using it in the Proxy Binding Update and Acknowledgment messages exchanged between the local mobility anchor to the mobile access gateway. This option can be used for exchanging the mobile node's home prefix and home address information.

The home network prefix Option has an alignment requirement of 8n+4. Its format is as follows:



Type

<IANA>

Length

8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. This field MUST be set to 18.

Reserved

This field is unused for now. The value MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

Prefix Length

8-bit unsigned integer indicating the prefix length of the IPv6 prefix contained in the option. If the prefix length is set to the value 128, indicates the presence of the mobile node's 128-bit home address.

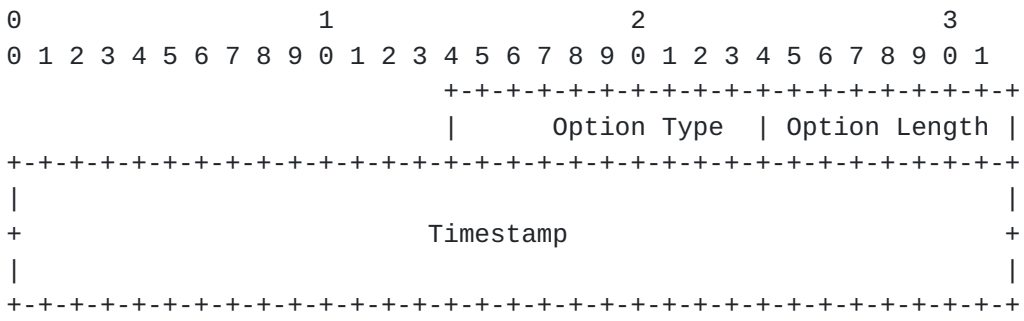
Home Network Prefix

A sixteen-byte field containing the Home Network Prefix

Figure 8: Home Network Prefix Option

8.4. Time Stamp Option

A new option, Time Stamp Option is defined for use in Proxy Binding Update and Acknowledgement messages. This option MUST be present in all Proxy Binding Update and Acknowledgement messages.



Type

<IANA>

Length

8-bit unsigned integer indicating the length in octets of the option, excluding the type and length fields. This field MUST be set to 18.

Timestamp

64-bit time stamp

Figure 9: Time Stamp Option

8.5. Status Codes

This document defines the following new Binding Acknowledgement status values:

145: Proxy Registration not supported by the local mobility anchor

146: Proxy Registrations from this mobile access gateway not allowed

147: No home address for this NAI is configured and the Home Network

Prefix Option not present in the Binding Update.

148: Invalid Time Stamp Option in the Binding Update

Status values less than 128 indicate that the Binding Update was processed successfully by the receiving nodes. Values greater than 128 indicate that the Binding Update was rejected by the local mobility anchor.

The value allocation for this usage needs to be approved by the IANA and must be updated in the IANA registry.

9. IANA Considerations

This document defines a new Mobility Header Option, the Mobile Home Network Prefix Option. This option is described in Section 8.3. The Type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options defined in [RFC-3775].

This document defines a new Mobility Header Option, the Time Stamp Option. This option is described in Section 8.4. The type value for this option needs to be assigned from the same numbering space as allocated for the other mobility options defined in [RFC-3775].

This document also defines new Binding Acknowledgement status values as described in Section 8.5. The status values MUST be assigned from the same space used for Binding Acknowledgement status values in [RFC-3775].

10. Security Considerations

The security threats against any general network-based mobility management protocol are covered in the document, Security Threats to Network-Based Localized Mobility Management [draft-ietf-netlmm-threats-04.txt]. This section analyses those vulnerabilities in the context of Proxy Mobile IPv6 protocol and covers all aspects around those identified vulnerabilities.

A compromised mobile access gateway can send Proxy Binding Update requests for mobile nodes that are not attached to its access link. This threat is similar to an attack on a typical routing protocol or equivalent to the compromise of a on-path router and hence this

threat exists in the network today and this specification does not make this vulnerability any worse than what it is. However, to eliminate this attack, the local mobility anchor can ensure that the mobile node is attached to the access link of the requesting mobile access gateway. This can be achieved using out of band mechanisms, such as from the mobile node's access authentication to the network and the specifics of how that is achieved is beyond the scope of this document.

This document does not cover the security requirements for authorizing the mobile node for the use of the access link. It is assumed that there are proper Layer-2 based authentication procedures, such as EAP, in place and will ensure the mobile node is properly identified and authorized before permitting it to access the network. It is further assumed that the same security mechanism will ensure the mobile session is not hijacked by malicious nodes on the access link.

This specification requires that all the signaling messages exchanged between the mobile access gateway and the local mobility anchor MUST be authenticated by IPsec [RFC-4301]. The use of IPsec to protect Mobile IPv6 signaling messages is described in detail in the HA-MN IPsec specification [RFC-3776] and the extension of that security model to Proxy Mobile IPv6 is covered in Section 4.0 of this document.

As described in the base Mobile IPv6 specification [RFC-3775], Section 5.1 both the mobile client (in this case, its the mobile access gateway) and the local mobility anchor MUST support and SHOULD use the Encapsulating Security Payload (ESP) header in transport mode and MUST use a non-NULL payload authentication algorithm to provide data origin authentication, data integrity and optional anti-replay protection.

The proxy solution allows one device creating a routing state for some other device at the local mobility anchor. It is important that the local mobility anchor has proper authorization services in place to ensure a given mobile access gateway is permitted to be a proxy for a specific mobile node. If proper security checks are not in place, a malicious node may be able to hijack a session or may do a denial-of-service attacks.

11. Acknowledgements

The authors would like to specially thank Julien Laganier, Christian Vogt, Pete McCann, Brian Haley and Ahmad Muhanna for their thorough

review of this document.

The authors would also like to thank the Gerardo Giaretta, Kilian Weniger, Alex Petrescu, Mohamed Khalil, Fred Templing, Nishida Katsutoshi, James Kempf, Vidya Narayanan, Henrik Levkowetz, Phil Roberts, Jari Arkko, Ashutosh Dutta, Hesham Soliman, Behcet Sarikaya, George Tsirtsis and many others for their passionate discussions in the working group mailing list on the topic of localized mobility management solutions. These discussions stimulated much of the thinking and shaped the draft to the current form. We acknowledge that !

The authors would also like to thank Ole Troan, Akiko Hattori, Perviz Yegani, Mark Grayson, Michael Hammer, Vojislav Vucetic, Jay Iyer and Tim Stammers for their input on this document.

12. References

12.1. Normative References

[RFC-1305] Mills, D., "Network Time Protocol (Version 3) Specification, Implementation", RFC 1305, March 1992.

[RFC-2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC-2461] Narten, T., Nordmark, E. and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC-2462] Thompson, S., Narten, T., "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[RFC-2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC-3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M.Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

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

[RFC-3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents",

RFC 3776, June 2004.

[RFC-4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6", RFC 4283, November 2005.

[RFC-4301] Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

[RFC-4306] Kaufman, C, et al, "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[draft-ietf-netlmm-nohost-req-05.txt] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Goals for Network-based Localized Mobility Management", October 2006.

[draft-ietf-netlmm-nohost-ps-05.txt] Kempf, J., Leung, K., Roberts, P., Nishida, K., Giaretta, G., Liebsch, M., "Problem Statement for Network-based Localized Mobility Management", September 2006.

[draft-ietf-netlmm-threats-04.txt] Vogt, C., Kempf, J., "Security Threats to Network-Based Localized Mobility Management", September 2006.

[draft-ietf-mip6-nemo-v4traversal-03.txt] Soliman, H. et al, "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", October 2006.

12.2. Informative References

[RFC-1332] McGregor, G., "The PPP Internet Protocol Control Protocol (IPCP)", RFC 1332, May 1992.

[RFC-1661] Simpson, W., Ed., "The Point-To-Point Protocol (PPP)", STD 51, RFC 1661, July 1994.

[RFC-2472] Haskin, D. and Allen, E., "IP version 6 over PPP", RFC 2472, December 1998.

[RFC-2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC-3041] Narten, T. and Draves, R., "Privacy Extensions for

Stateless Address Autoconfiguration in IPv6", RFC 3041, January 2001.

[RFC-3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC-3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[draft-iab-multilink-subnet-issues-03.txt] Thaler, D., "Multilink Subnet Issues", January 2006.

[draft-ietf-dna-protocol-03] Kempf, J., et al "Detecting Network Attachment in IPv6 Networks (DNAv6)", draft-ietf-dna-protocol-03, October 2006.

[draft-ietf-mip6-ikev2-ipsec-08] Devarapalli, V. and Dupont, F., "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", December 2006.

Appendix A. Proxy Mobile IPv6 interactions with AAA Infrastructure

Every mobile node that roams in a proxy Mobile IPv6 domain, would typically be identified by an identifier, MN-Identifier, and that identifier will have an associated policy profile that identifies the mobile node's home network prefix, permitted address configuration modes, roaming policy and other parameters that are essential for providing network-based mobility service. This information is typically configured in AAA. It is possible the home network prefix is dynamically allocated for the mobile node when it boots up for the first time in the network, or it could be a statically configured value on per mobile node basis. However, for all practical purposes, the network entities in the proxy Mobile IPv6 domain, while serving a mobile node will have access to this profile and these entities can query this information using RADIUS/DIAMETER protocols.

Appendix B. Supporting Shared-Prefix Model using DHCPv6

For supporting shared-prefix model, i.e, if multiple mobile nodes are configured with a common IPv6 network prefix, as in Mobile IPv6 specification, it is possible to support that configuration under the following guidelines:

The mobile node is allowed to use statefull address configuration

using DHCPv6 for obtaining its address configuration. The mobile nodes is not allowed to use any of the stateless autoconfiguration techniques. The permitted address configuration models for the mobile node on the access link can be enforced by the mobile access gateway by setting the relevant flags in the Router Advertisements, as per ND Specification, [RFC-2461]

The Home Network Prefix Option that is sent by the mobile access gateway in the Proxy Binding Update message, must contain the 128-bit host address that the mobile node obtained via DHCPv6.

Routing state at the mobile access gateway:

For all IPv6 traffic from the source MN-HoA::/128 to destination 0::/0, route via tunnel0, next-hop LMAA, where tunnel0 is the MAG to LMA tunnel.

Routing state at the local mobility anchor:

For all IPv6 traffic to destination MN-HoA::/128, route via tunnel0, next-hop Proxy-CoA, where tunnel0 is the LMA to MAG tunnel.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Kent Leung
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: kleung@cisco.com

Vijay Devarapalli
Azaire Networks
4800 Great America Pkwy
Santa Clara, CA 95054
USA

Email: vijay.devarapalli@azairenet.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA

Email: kchowdhury@starentnetworks.com

Basavaraj Patil
Nokia Siemens Networks
6000 Connection Drive
Irving, TX 75039
USA

Email: basavaraj.patil@nsn.com

Full Copyright Statement

Intellectual Property

Acknowledgment

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