| | |
|---|---|
| Network Working Group | G. Tsirtsis |
| Internet-Draft | V. Park |
| Intended status: Standards Track | Qualcomm |
| Expires: July 19, 2009 | H. Soliman |
| | Elevate Technologies |
| | January 15, 2009 |


TOC

**Dual Stack Mobile IPv4**
**draft-ietf-mip4-dsmipv4-10.txt**

### Status of this Memo



### Copyright Notice



### Abstract


This specification provides IPv6 extensions to the Mobile IPv4 protocol. The extensions allow a dual stack node to use IPv4 and IPv6 home addresses as well as to move between IPv4 and dual stack network infrastructures.

## Table of Contents



## 1. Requirements Notation

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

## 2. Introduction

TOC

Mobile IPv4 [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.) allows a mobile node with an IPv4 address to maintain communications while moving in an IPv4 network.
Extensions defined in this document allow a node that has IPv4 and IPv6 addresses [RFC2460] (Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," December 1998.) to maintain communications through any of its addresses while moving in IPv4 or dual stack networks.
Essentially, this specification separates the Mobile IPv4 signaling from the IP version of the traffic it tunnels. Mobile IPv4 with the present extensions remains a signaling protocol that runs over IPv4, and yet can set-up both IPv4 and IPv6 tunnels over IPv4.
The aim is two-fold:

> On one hand, Mobile IPv4 with the present extensions becomes a useful transition mechanism, allowing automated but controlled tunneling of IPv6 traffic over IPv4 tunnels. Dual stack nodes in dual stack home networks can now roam to and from legacy IPv4 networks, while IPv4 mobile nodes and networks can migrate to IPv6 without changing mobility management, and without upgrading all network nodes to IPv6 at once.
>
> On the other hand, and more importantly, it allows dual stack mobile nodes and networks to utilize a single protocol for the movement of both IPv4 and IPv6 stacks in the network topology.

Note that features like Mobile IPv6 [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," June 2004.) style route optimization will not be possible with this solution as it still relies on Mobile IPv4 signaling, which does not provide route optimization.

---

### 2.1. Goals

TOC

> **a.** The solution supports the registration of IPv6 home prefix(s) in addition to regular IPv4 home address registration
>
> **b.** The solution supports static and dynamic IPv6 prefix delegation

---

### 2.2. Non-Goals

TOC

a. The solution does not provide support for IPv6 care-of address registration

### 2.3. Implicit and Explicit Modes

TOC

As defined in NEMO [RFC3963] (Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, “Network Mobility (NEMO) Basic Support Protocol,” January 2005.), this specification also supports two modes of operation; the implicit mode and the explicit mode.

In the implicit mode, the mobile node does not include any IPv6 prefix request extensions in the Registration Request. The home agent can use any mechanism (not defined in this document) to determine the IPv6 prefix(es) owned by the mobile node and to set up forwarding for these prefixes. In this mode of operation all traffic to and from the IPv6 prefixes MUST be encapsulated over the IPv4 tunnel between the mobile node's IPv4 home address and the IPv4 address of the home agent, and as such it is transparent to any foreign agent in the path. This IPv4 tunnel is established by mechanisms that are out of the scope of this document on both the mobile node and home agent when operating in the implicit mode.

In the explicit mode, IPv6 bindings are signalled explicitly. The mobile node includes one or more IPv6 prefix request extensions in the Registration Request, while the home agent returns corresponding IPv6 prefix reply extensions to accept/reject the IPv6 bindings. Additionally, in the explicit mode, the mobile node (when co-located mode of operation is used) can indicate whether IPv6 traffic should be tunneled to the care-of address or the home address of the mobile node. The rest of this specification is primarily defining the explicit mode.

## 3. Extension Formats

TOC

The following extensions are defined according to this specification.

### 3.1. IPv6 Prefix Request Extension

TOC

A new skippable extension to the Mobile IPv4 registration request message in accordance to the short extension format of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) is defined here.

This extension contains a mobile IPv6 network prefix and its prefix length.

```
 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 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |    Sub-Type    | Prefix Length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                   Mobile IPv6 Network Prefix                  +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure 1: IPv6 Prefix Request Extension**

Type

> TBD (DSMIPv4 Extension)(skippable type to be assigned by IANA)

Length

> 18

Sub-Type

> 1 (IPv6 Prefix Request)

Prefix Length

> A sixteen-byte field containing the Mobile IPv6 Network Prefix; all insignificant (low-order) bits (beyond the Prefix Length) MUST be set to 0 by the originator of the option and ignored by the receiver

Mobile IPv6 Network Prefix

> A sixteen-byte field containing the Mobile IPv6 Network Prefix

TOC

### 3.2. IPv6 Prefix Reply Extension

A new skippable extension to the Mobile IPv4 registration reply message in accordance to the short extension format of [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.) is defined here.

This extension defines a mobile IPv6 network prefix and its prefix length, as well as a code.

```
 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 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |   Sub-Type    |     Code      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Prefix Length |   Reserved    |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               +
|                                                               |
+                                                               +
|                                                               |
+                   Mobile IPv6 Network Prefix                  +
|                                                               |
+                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure 2: IPv6 Prefix Reply Extension**

Type

> TBD (DSMIPv4 Extension)(skippable type to be assigned by IANA)

Length

> 20

Sub-Type

> 2 (IPv6 Prefix Reply)

Code

> A value indicating the result of the registration request with respect to the IPv6 home prefix registration. See below for currently defined Codes.

Prefix Length

> Indicates the prefix length of the prefix included in the Mobile IPv6 Network Prefix field. A value of 255 indicates that a link local address is included in the Mobile IPv6 Network Prefix field.

Reserved

> Set to 0 by the sender, ignored by the receiver

Mobile IPv6 Network Prefix

> A sixteen-byte field containing the Mobile IPv6 Network Prefix; all insignificant (low-order) bits (beyond the Prefix Length) MUST be set to 0 by the originator of the option and ignored by the receiver

The following values are defined for use as a Code value in the above extension

> 0 registration accepted, IPv6 to be tunneled to HoA
>
> 1 registration accepted, IPv6 to be tunneled to CoA
>
> 8 registration rejected, reason unspecified
>
> 9 registration rejected, administratively prohibited

Note that a registration reply that does not include an IPv6 prefix reply extension, when received in response to a registration request carrying at least one instance of the IPv6 prefix request extension, indicates that the home agent does not support IPv6 extensions and thus has ignored such extensions in the registration request.

---

### 3.3. IPv6 Tunneling Mode Extension

TOC

A new skippable extension to the Mobile IPv4 registration request message in accordance to the short extension format of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.) is defined here.

---

By including this extension in a registration request the sender indicates that IPv6 traffic can be tunneled to the mobile node's CoA.

```
 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 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |    Sub-Type   |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

**Figure 3: IPv6 Tunneling Mode Extension**

Type

> TBD (DSMIPv4 Extension) (skippable type to be assigned by IANA)

Length

> 2

Sub-Type

> 3 (IPv6 Tunneling Mode)

Reserved

> Set to 0 by the sender, ignored by the receiver

## 4. Mobile IP Registrations

TOC

### 4.1. Registration Request

TOC

A mobile node MAY include in a registration request one or more IPv6 prefix request extensions defined in this specification.
A mobile node MAY also include exactly one IPv6 tunneling mode extension when it uses the co-located care-of address mode of [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
When IPv6 prefix and/or IPv6 tunneling mode extensions are used by the mobile IP client, they MUST be placed after the registration request header and before the mobile – home authentication extension so they MUST be included in the computation of any authentication extension.

### 4.2. Registration Reply

TOC

The mechanism described in this specification depends on skippable extensions. For that reason, a registration reply that does not include an IPv6 prefix reply extension, in response to a registration request including an IPv6 prefix request extension, indicates that the home agent does not support IPv6 extensions and has ignored the request.
If an IPv6 prefix reply extension is included in a registration reply, then the extension indicates the success or failure of the IPv6 prefix registration. The IPv6 prefix reply extension does not affect in any way the code value in the registration reply header but it is superseded by it. In other words if the code field in the registration reply header is set to a reject code, then all IPv6 prefix request extensions are also rejected. If the code field in the registration reply header, however, is set to an accept code, then an IPv6 prefix reply extension with a code field set to a reject code only rejects the binding for the specific IPv6 prefix indicated in the same extension. Note that a rejecting IPv6 prefix reply extension has the same effect as not including such an extension at all, in the sense that in both cases the mobile node must act as if the corresponding IPv6 prefix request extension included in the registration request was rejected. Of course, the inclusion of the IPv6 prefix reply extension allows the home agent to indicate why a given IPv6 prefix request extension was rejected. A detailed description of how the mobile node handles different IPv6 prefix reply extension code values and the absence of IPv6 prefix reply extensions is given in Section 4.5 (Mobile Node Considerations).

---

### 4.3. Home Agent Considerations

TOC

The dual stack home agent defined in this specification is a Mobile IPv4 home agent in that, it MUST operate as defined in MIPv4 [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). In addition to that, the following mechanisms are defined in this specification.
For each IPv6 prefix request extension included in a valid registration request, a home agent that supports this specification SHOULD include a corresponding IPv6 prefix reply extension in the registration reply message. The home agent MUST NOT include more than one IPv6 prefix reply extension for the same prefix. For each accepted IPv6 prefix the home agent MUST decide the tunneling mode it is going to use and set the code field of the IPv6 prefix reply extension to the appropriate value. The IPv6 prefix field of each of the IPv6 prefix reply extensions included in the registration reply MUST match the IPv6

prefix field of an IPv6 prefix request extension included in the corresponding registration request message.
When the home agent sends a successful registration reply to the mobile node, with the code field of a corresponding IPv6 prefix reply extension set to one of the "registration accepted" values, the home agent indicates that the IPv6 prefix is registered for the lifetime granted for the binding. It also indicates the tunneling mode used i.e., tunneling to home address or care-of address, based on the value of the code field used in the IPv6 prefix reply extension.
Note that since only IPv6 prefixes (and not addresses) are supported by this specification, there is no need for Duplicate Address Detection. The home agent, however, MUST check that registered prefixes are not overlapping so that all addresses under each registered prefix belong to a single mobile node at any one time. These prefixes MUST NOT appear as on-link to any other node (e.g., via Router Advertisements).

---

### 4.3.1. IPv6 Reachability

TOC

For each registered IPv6 prefix, the home agent MUST advertise its reachability as defined in NEMO [RFC3963] (Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, “Network Mobility (NEMO) Basic Support Protocol,” January 2005.), section 6.3.

---

### 4.3.2. Processing intercepted IPv6 Packets

TOC

A dual stack home agent that supports the IPv6 extensions defined in this specification, MUST keep track of the following IPv6 related state for the mobile nodes it supports, in addition to the state defined in [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).
- Registered IPv6 prefix(es) and prefix length(s)
- Tunneling mode for IPv6 traffic:

> - Tunnel to IPv4 HoA and accept IPv6 tunneled from IPv4 HoA.
>
> - Tunnel to CoA and accept IPv6 tunneled from CoA.

When IPv6 traffic is encapsulated over the tunnel between the HA and the mobile node's care-off address, the tunneling mechanism used should be the same as the mechanism negotiated by the Mobile IP header as defined in MIPv4 [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). In that case, when IPinIP encapsulation is negotiated, IPv6 is tunneled over IPv4 according to [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.). GRE also allow tunneling of IPv6

packets by setting the Protocol Type [RFC2784] (Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, “Generic Routing Encapsulation (GRE),” March 2000.) field, to the appropriate payload type defined for IPv6 by IANA. Minimal Encapsulation [RFC2004] (Perkins, C., “Minimal Encapsulation within IP,” October 1996.) cannot be used, since the second (inner) IP header is IPv6, which is not supported by [RFC2004] (Perkins, C., “Minimal Encapsulation within IP,” October 1996.).
When IPv6 traffic is encapsulated over the tunnel between the HA and the mobile node's home address, IPv6 is always tunneled over IPv4 according to [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.).The resulting IPv4 packet is then delivered just like any other IPv4 packet addressed to the IPv4 HoA (using the tunneling for normal IPv4 traffic, possibly going via FA).
Tunneling mode selection for IPv6 traffic depends on the following parameters in a successful registration request:
1) A registration request is received with one or more IPv6 prefix request extensions. An IPv6 tunneling mode extension is not included.

> All IPv6 packets destined to the registered IPv6 prefix(es) MUST be tunneled by the home agent to the registered IPv4 home address of the mobile node. The home agent first encapsulates the IPv6 packet, addressing it to the mobile node's IPv4 home address, and then tunnels this encapsulated packet to the foreign agent. This extra level of encapsulation is required so that IPv6 routing remains transparent to a foreign agent that does not support IPv6. When received by the foreign agent, the unicast encapsulated packet is detunneled and delivered to the mobile node in the same way as any other packet. The mobile node must decapsulate the received IPv4 packet in order to recover the original IPv6 packet.
>
> Additionally, the home agent MUST be prepared to accept reverse tunneled packets from the IPv4 home address of the mobile node encapsulating IPv6 packets sent by that mobile node.

2) A registration request is received with one or more IPv6 prefix request extensions. An IPv6 tunneling mode extension is included.

> All IPv6 packets destined to the registered IPv6 prefix(es) SHOULD be tunneled by the home agent to the registered care-of address of the mobile node. Additionally, the home agent SHOULD be prepared to accept reverse tunneled packets from the care-of address of the mobile node encapsulating IPv6 packets sent by that mobile node. The home agent MAY ignore the presence of the IPv6 tunneling mode extension and act as in case (1) above.

The home agent MUST check that all inner IPv6 packets received from the mobile node over a tunnel with the mobile node's home address or the care-of address as the outer source address, include a source address

that falls under the registered IPv6 prefix(es) for that mobile node. If the source address of the outer header of a tunneled packet is not the registered IPv4 care-of address or the registered IPv4 home addresses, the packet SHOULD be dropped. If the source address of the inner header of an tunneled packet does not match any of the registered prefixes the packet SHOULD be dropped.
Multicast packets addressed to a group to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.

---

### 4.3.3. IPv6 Multicast Membership Control

TOC

IPv6 multicast membership control is provided as defined in MIPv6 [RFC3775] (Johnson, D., Perkins, C., and J. Arkko, “Mobility Support in IPv6,” June 2004.), Section 10.4.3. The only clarification required for the purpose of this specification is that all MLD [RFC2710] (Deering, S., Fenner, W., and B. Haberman, “Multicast Listener Discovery (MLD) for IPv6,” October 1999.) or MLDv2 [RFC3810] (Vida, R. and L. Costa, “Multicast Listener Discovery Version 2 (MLDv2) for IPv6,” June 2004.) messages between the mobile node and the home agent MUST be tunneled over an IPv4 tunnel between the mobile node's IPv4 home address and the home agent's IPv4 address, bypassing the foreign agent. Note that if tunneling to the care-of address has been negotiated for other traffic, then the rest of the traffic continues using this tunnel.

---

### 4.4. Foreign Agent Considerations

TOC

This specification does not afect the operation of the foreign agent.

---

### 4.5. Mobile Node Considerations

TOC

A dual stack mobile node that supports the extensions described in this document MAY use these extensions to register its IPv6 prefix(es) while moving between access routers.
The mobile node MAY include one or more IPv6 prefix request extension(s) in the registration request.
In this case the mobile MUST take the following action depending on the extensions included in the registration reply it receives in response to the registration request:
1) The registration reply does not include any IPv6 prefix reply extensions.

> The mobile node MUST assume that the home agent does not support the extensions defined in this specification. The mobile node SHOULD continue to operate according to MIPv4 [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.).

2) The registration reply includes one or more IPv6 prefix reply extensions.

> The mobile node MUST match each IPv6 prefix reply extension with one of the IPv6 prefix request extensions earlier included in the corresponding registration request message.
>
> If a matching IPv6 prefix reply extension is not included for one or more of corresponding IPv6 prefix request extensions included in the registration request message, the mobile node MUST assume that these IPv6 prefixes are rejected.
>
> For each matching IPv6 prefix reply extension the mobile node MUST inspect the code field. If the field is set to a rejection code then the corresponding IPv6 prefix registration has been rejected. If the code field is set to an acceptance code then the corresponding IPv6 prefix registration has been accepted.
>
> If the code field is set to “0” then the mobile node MUST be prepared to send/receive IPv6 packets encapsulated in the bidirectional tunnel between the home agent address and the registered IPv4 home address of the mobile node.
>
> If the code field is set to “1” then the mobile node MUST act as follows:
>
> - Assuming the co-located care-of address mode is used, the mobile node MUST be prepared to send/receive IPv6 packets over the bidirectional tunnel between the home agent address and its co-located care-of address. Otherwise the mobile node SHOULD act as in the case where the code field is set to "0".

The mobile node SHOULD include exactly one IPv6 tunneling mode extension if it uses the co-located care-of address model and it wants to request that IPv6 packets are tunneled to its co-located care-of address. If the mobile node uses the co-located care-of address model but it does not include the IPv6 tunneling mode extension, the home agent will tunnel IPv6 traffic to the mobile node’s IPv4 home address. The mobile node MUST NOT include an IPv6 tunneling mode extension if it uses the foreign agent care-of address mode of operation. Note that if the mobile node includes an IPv6 tunneling mode extension in this case, IPv6 packets could be tunneled to the FA by the HA. The FA is then likely to drop them since it will not have appropriate state to process them.

### 4.6. Tunneling Impacts

TOC

When IPv6 runs over an IPv4 tunnel, the IPv6 tunnel end points can treat the IPv4 tunnel as a single hop link as defined in [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.). The two tunnel end points, e.g., mobile node and home agent, MUST configure link local IPv6 addresses as defined in [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.), section 3.7, while they MUST also adhear to the neighbor discovery requirements of the same specification, section 3.8 and the hop limit requirements of section 3.3.

With respect to the Tunnel MTU an implementation MUST support the Static Tunnel MTU approach as defined in [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.), section 3.2. Implementation and use of the Dynamic Tunnel MTU method defined in the same section of [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.) is OPTIONAL.

To accommodate traffic that uses Explicit Congestion Notification (ECN), it is RECOMMENDED that the ECN and DSCP information is copied between the inner and outer header as defined in [RFC3168] (Ramakrishnan, K., Floyd, S., and D. Black, “The Addition of Explicit Congestion Notification (ECN) to IP,” September 2001.) and [RFC2983] (Black, D., “Differentiated Services and Tunnels,” October 2000.). It is RECOMMENDED that the full-functionality option defined in section 9.1.1 of [RFC3168] (Ramakrishnan, K., Floyd, S., and D. Black, “The Addition of Explicit Congestion Notification (ECN) to IP,” September 2001.) is used to deal with ECN

### 4.7. IPv6 Prefixes

TOC

An implementation can use any number of mechanisms to allocate IPv6 prefixes to a mobile node. Once one or more IPv6 prefixes are allocated, they can be registered using the extensions and mechanism already described in this specification.

How a home agent decides to accept an IPv6 prefix for a given mobile node is out of scope of this specification. Local configuration or external authorization via an authorization system e.g., Diameter [RFC3588] (Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, “Diameter Base Protocol,” September 2003.), or other mechanisms may be used to make such determination.

### 4.7.1. Dynamic IPv6 Prefix Delegation

TOC

A dual stack mobile node MAY use prefix delegation as defined in DHCPv6 Prefix Delegation [RFC3633] (Troan, O. and R. Droms, “IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6,” December 2003.) to get access to IPv6 prefixes. In that case, if the mobile node is not directly attached to its home agent, the mobile node MUST first register its IPv4 home address as per MIPv4 [RFC3344] (Perkins, C., “IP Mobility Support for IPv4,” August 2002.). When that is done the mobile node can generate a link local IPv6 address as per [RFC4213] (Nordmark, E. and R. Gilligan, “Basic Transition Mechanisms for IPv6 Hosts and Routers,” October 2005.), section 3.7. The mobile node then sends registration request to its home agent, including an IPv6 prefix request extension with prefix length field set to 255 and by setting the mobile IPv6 network prefix field to the localy generated link local address. If the registration reply message includes an IPv6 prefix reply extension with the code field set to a success code the mobile node can use the tunnel to send and receive IPv6 link local packets. The mobile node can now send DHCPv6 messages according to [RFC3633] (Troan, O. and R. Droms, “IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6,” December 2003.). All IPv6 messages at this stage MUST be tunneled over the IPv4 tunnel between the mobile node's IPv4 home address and the home agent's IPv4 address.
Once prefixes are delegated, and assuming explicit mode is used, the mobile node SHOULD send a registration request with appropriate IPv6 prefix request extensions to the home agent to register the delegated prefixes.

---

### 4.8. Deregistration of IPv6 Prefix

TOC

The mobile IP registration lifetime included in the registration request header is valid for all the bindings created by the registration request, which may include bindings for IPv6 prefix(es).
A registration request with a zero lifetime can be used to remove all bindings from the home agent.
A re-registration request with non-zero lifetime can be used to deregister some of the registered IPv6 prefixes by not including corresponding IPv6 prefix request extensions in the registration request message.

---

TOC

### 4.9.  Registration with a private CoA

If the care-of address is a private address then Mobile IP NAT Traversal as [RFC3519] (Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices," April 2003.) MAY be used in combination with the extensions described in this specification. In that case, to transport IPv6 packets, the next header field of the Mobile Tunnel Data message header [RFC3519] (Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices," April 2003.) MUST be set to the value for IPv6. Note that in that case the encapsulation field of the UDP Tunnel Request Extension defined in [RFC3519] (Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices," April 2003.) MUST be set to zero.

---

## 5.  Security Considerations

TOC

This specification operates in the security constraints and requirements of [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.). It extends the operations defined in [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.) for IPv4 home addresses to cover home IPv6 prefixes and provides the same level of security for both IP address versions.
Home agents MUST perform appropriate checks for reverse tunneled IPv6 packets similar to what is defined in [RFC3024] (Montenegro, G., "Reverse Tunneling for Mobile IP, revised," January 2001.) for IPv4 packets. The check defined in [RFC3024] (Montenegro, G., "Reverse Tunneling for Mobile IP, revised," January 2001.) requires that the outer header's source address is set to a registered care-of address for the mobile node and as such the same check protects from attacks whether the encapsulated (inner) header is IPv4 or IPv6.
In addition to that, the home agent MUST check that the source address of the inner header is a registered IPv4 home address or IPv6 prefix for this mobile node. If that is not the case, the home agent SHOULD silently discard the packet and log the event as a security exception.
Security devices should look for IPv6 packets encapsulated over IPv4 either directly to the mobile node's care-of address or via double encpasulation first to the mobile node's IPv4 home address and then to the mobile node's care-of addres. Interactions with Mobile IPv4 and IPsec have been covered elsewhere, for instance in [RFC5265] (Vaarala, S. and E. Klovning, "Mobile IPv4 Traversal across IPsec-Based VPN Gateways," June 2008.) and [RFC5266] (Devarapalli, V. and P. Eronen, "Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE)," June 2008.).

---

## 6. IANA Considerations

TOC

This specification requires the allocation of a new type number for DSMIPv4 extensions, from the space of numbers for skippable mobility extensions (i.e., 128-255), defined for Mobile IPv4 [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.) at http://www.iana.org/assignments/mobileip-numbers, under extensions appearing in Mobile IP control messages..

This specification also creates a new subtype space for the type number of this extension. The subtype values 1, 2 and 3 are defined in this specification, while the rest of the sub-types are reserved and available for allocation based on expert review.

Finally, this specification creates a new space for the code field of the IPv6 prefix reply extension. Values 0, 1, 8, and 9 are defined in this specification. Values 2-7 are reserved for accept codes and values 10-255 are reserved for reject codes.

Similar to the procedures specified for Mobile IPv4 [RFC3344] (Perkins, C., "IP Mobility Support for IPv4," August 2002.) number spaces, future allocations from the two number spaces require expert review [RFC5226] (Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," May 2008.).

---

## 7. Acknowledgements

TOC

Thanks to Pat Calhoun, Paal Engelstad, Tom Hiller and Pete McCann for earlier work on this subject. Thanks also to Alex Petrescu for various suggestions. Special thanks also to Sri Gundavelli and Kent Leung for their thorough review and suggestions.

---

## 8. References

TOC

---

### 8.1. Normative References

TOC


| | |
|---|---|
| [RFC2119] | Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML). |
| [RFC2460] | Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, December 1998 (TXT, HTML, XML). |
| [RFC3024] | |

| | |
|---|---|
| | Montenegro, G., "Reverse Tunneling for Mobile IP, revised," RFC 3024, January 2001 (TXT). |
| [RFC3344] | Perkins, C., "IP Mobility Support for IPv4," RFC 3344, August 2002 (TXT). |
| [RFC3519] | Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices," RFC 3519, April 2003 (TXT). |
| [RFC3633] | Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6," RFC 3633, December 2003 (TXT). |
| [RFC3775] | Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004 (TXT). |
| [RFC3963] | Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," RFC 3963, January 2005 (TXT). |
| [RFC4213] | Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers," RFC 4213, October 2005 (TXT). |
| [RFC5226] | Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," BCP 26, RFC 5226, May 2008 (TXT). |

### 8.2. Informative References

TOC

| | |
|---|---|
| [RFC2004] | Perkins, C., "Minimal Encapsulation within IP," RFC 2004, October 1996 (TXT, HTML, XML). |
| [RFC2710] | Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6," RFC 2710, October 1999 (TXT). |
| [RFC2784] | Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)," RFC 2784, March 2000 (TXT). |
| [RFC2983] | Black, D., "Differentiated Services and Tunnels," RFC 2983, October 2000 (TXT). |
| [RFC3168] | Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP," RFC 3168, September 2001 (TXT). |
| [RFC3588] | Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol," RFC 3588, September 2003 (TXT). |
| [RFC3810] | Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6," RFC 3810, June 2004 (TXT). |
| [RFC5265] | Vaarala, S. and E. Klovning, "Mobile IPv4 Traversal across IPsec-Based VPN Gateways," RFC 5265, June 2008 (TXT). |
| [RFC5266] | |

| | |
|---|---|
| | Devarapalli, V. and P. Eronen, “Secure Connectivity and Mobility Using Mobile IPv4 and IKEv2 Mobility and Multihoming (MOBIKE),” BCP 136, RFC 5266, June 2008 (TXT). |

## Authors' Addresses

TOC

| | |
|---|---|
| | George Tsirtsis |
| | Qualcomm |
| Email: | tsirtsis@googlemail.com |
| | |
| | Vincent Park |
| | Qualcomm |
| Phone: | +908-947-7084 |
| Email: | vpark@qualcomm.com |
| | |
| | Hesham Soliman |
| | Elevate Technologies |
| Phone: | +614-111-410-445 |
| Email: | hesham@elevatemobile.com |