Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 16, 2008

G. Tsirtsis
V. Park
Qualcomm
H. Soliman
Elevate Technologies

February 13, 2008

Dual Stack Mobile IPv4
draft-ietf-mip4-dsmipv4-06.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

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].

2. Introduction

Mobile IPv4 [RFC3344] 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] 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] 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

a. The solution supports the registration of IPv6 home address(es) and/or prefix(s) in addition to regular IPv4 home address registration

b. The solution supports static and dynamic IPv6 home address(s)/ prefix(s) allocations

c. The solution supports the above registrations with and without FA support

2.2. Non-Goals

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

2.3. Implicit and Explicit Modes

As defined in NEMO [RFC3963], 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 address 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) or the foreign agent (when present) can indicate whether IPv6 traffic should be tunneled to the care-of address of the home address of the mobile node.

The rest of this specification is primarily defining the explicit mode.

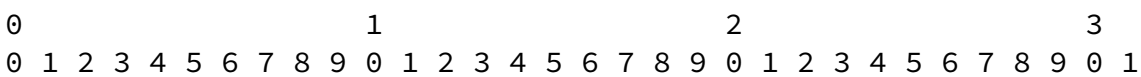
3. Extension Formats

The following extensions are defined according to this specification.

3.1. IPv6 Prefix Request Extension

A new skippable extension to the Mobile IPv4 registration request message in accordance to the short extension format of [RFC3344] is defined here.

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



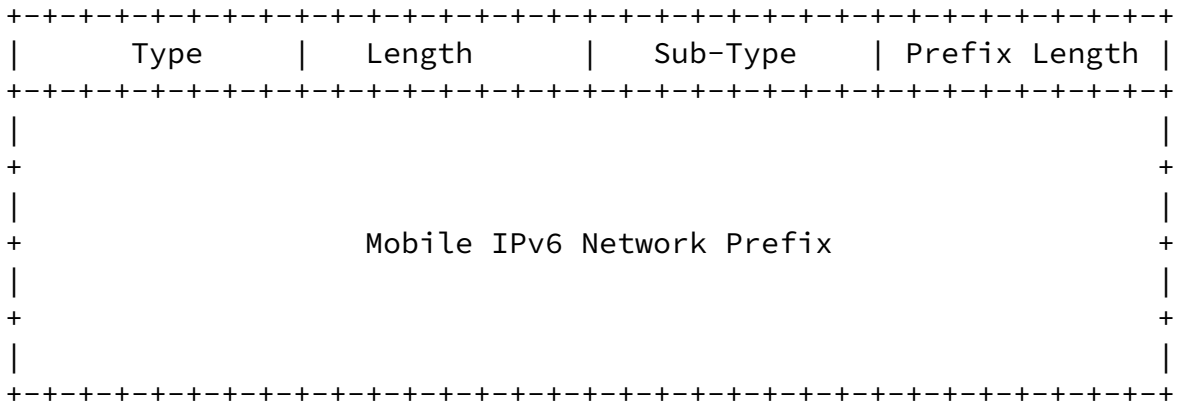


Figure 1: IPv6 Prefix Request Extension

Type

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

Length

18

Sub-Type

1 (IPv6 Prefix Request)

Prefix Length

Indicates the prefix length of the prefix included in the Mobile IPv6 Network Prefix field

Mobile IPv6 Network Prefix

A sixteen-byte field containing the Mobile IPv6 Network Prefix

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] is defined here.

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

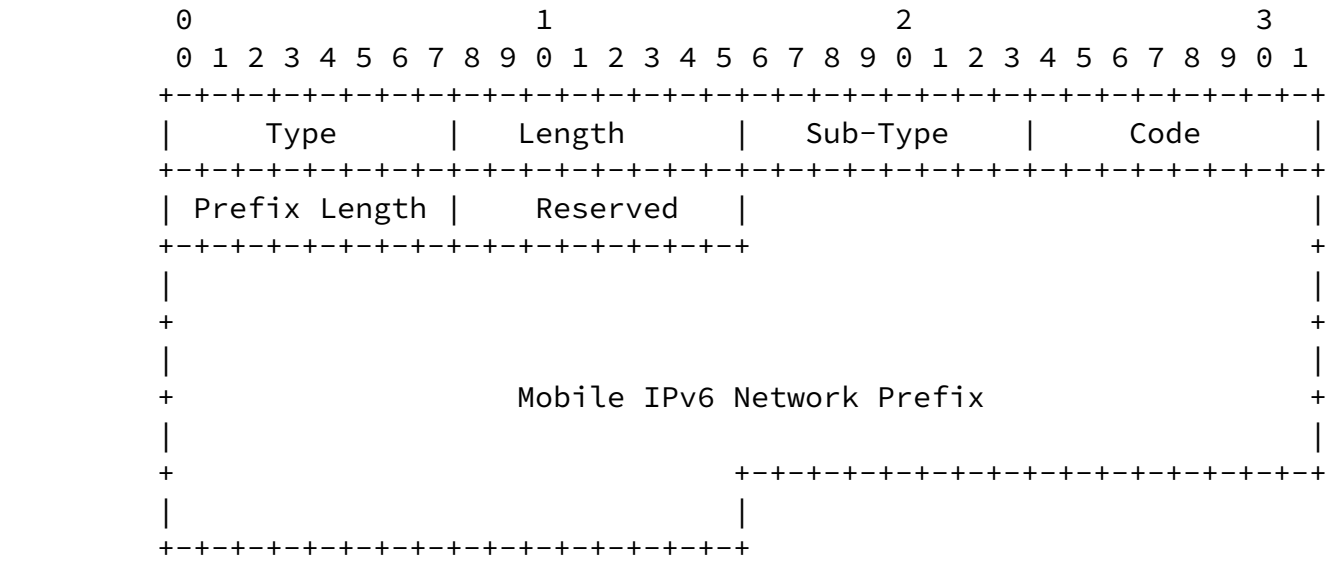


Figure 2: IPv6 Prefix Reply Extension

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 address registration. See below for currently defined Codes.

Prefix Length

Indicates the prefix length of the prefix 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

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

10 registration rejected, not home subnet

11 registration rejected, Duplicate Address Detection failed

Note that a registration reply that does not include an IPv6 Prefix Reply 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

A new skippable extension to the Mobile IPv4 registration request message in accordance to the short extension format of [RFC3344] is defined here.

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

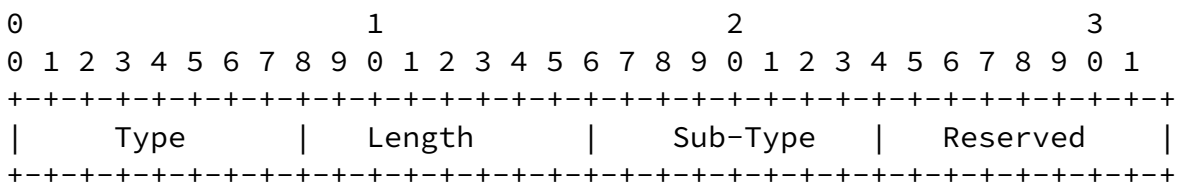


Figure 3: IPv6 Tunneling Mode Extension

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

4.1. Registration Request

A mobile node MAY include one or more IPv6 Prefix Request extensions defined in this specification in a registration request.

A mobile node MAY include exactly one IPv6 tunneling mode extension when it uses the co-located care-of address mode of [RFC3344].

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.

A foreign agent MAY include exactly one IPv6 tunneling mode extension, defined in this specification, in a registration request when a mobile node registers using the care-of address mode via the foreign agent.

When the IPv6 tunneling mode extension is used by a foreign agent it MUST be placed after the mobile - home authentication extensions and before the foreign - home authentication extension so they MUST be included in the computation of the foreign - home authentication extension when one exists.

4.2. Registration Reply

The mechanism described in the 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 that included 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 and foreign agent 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. Consequently, home agent implementations of this specification SHOULD include, in the registration reply messages, an IPv6 Prefix Reply extension for each IPv6 Prefix Request extension included in the corresponding registration request message. 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.

4.3. Home Agent Considerations

The dual stack home agent defined in this specification is a Mobile IPv4 [RFC3344] Home Agent, in that it MUST operate as defined in MIPv4 [RFC3344]. In addition to that the following mechanism 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 included 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 extensions

included in the corresponding registration request message.

If the IPv6 home address included in an IPv6 Prefix Request extension is not an on-link IPv6 address with respect to the home agent's current Prefix List or a prefix it is configured to serve, the home agent MUST reject the IPv6 Prefix Request extension and SHOULD return an IPv6 Prefix Reply extension with rejection code "registration rejected, not home subnet" in the registration reply to the mobile node.

When the IPv6 Prefix Request extension contains a /128 IPv6 address and unless this home agent already has a binding for the given IPv6 address indicated, the home agent MUST perform Duplicate Address Detection [RFC4862] on the mobile node's home IPv6 link before returning a registration reply. This ensures that no other node on the home link is using the IPv6 home address. Duplicate address

detection is not required when the IPv6 Prefix Request extension contains a prefix. If this Duplicate Address Detection fails for the given IPv6 home address or an associated link local address, then the home agent MUST reject the IPv6 Prefix Request extension and SHOULD return a registration reply to the mobile node, in which the code field of the corresponding IPv6 Prefix Reply extension is set to "registration rejected, Duplicate Address Detection failed".

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 assures the mobile node that its IPv6 address(es) will be kept unique by the home agent for as long as the lifetime is 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 for IPv6 prefixes (rather than addresses), the home agent does not have to perform Duplicate Address Detection but it MUST check that allocated prefixes are not overlapping so that all addresses under each allocated prefix are allocated only to a single mobile node at any one time.

4.3.1. IPv6 Packet Processing

Dual stack home agents MUST use Proxy Neighbor Discovery [RFC4861] on behalf of the nodes they serve. This allows the home agent to receive IPv6 packets addressed to the mobile node's registered IPv6 address(es).

In this respect, the dual stack home agent MUST act as defined in MIPv6 [RFC3775], Section 10.4.1. in order to intercept IPv6 packets for the mobile nodes it serves.

The home agent MUST advertise reachability for the registered prefixes as defined in NEMO [RFC3963], section 6.3.

4.3.2. Processing intercepted IPv6 Packets

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].

- 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]. In that case, when IPinIP encapsulation is negotiated, IPv6 is tunneled over IPv4 according to[RFC4213]. GRE and Minimal Encapsulation techniques also allow tunneling of IPv6 packets by setting the Protocol Type [RFC2784] and Protocol [RFC2004] fields to appropriate payload type defined for IPv6 by IANA. When, however, 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], no matter what tunneling mechanism is negotiated in MIPv4 signaling.

A home agent that supports this specification MUST be able to defend

IPv4 and IPv6 addresses registered by mobile nodes according to mechanisms described in MIPv4 [RFC3344] and MIPv6 [RFC3775] specifications.

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. The home agent first encapsulates the IPv6 packetm 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 encapsulating IPv6 packets sent by that mobile.

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 home address(s) 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 encapsulating IPv6 packets sent by that mobile. The home agent MAY ignore the presence of the IPv6 tunneling mode extension and act as in case (1) above.

Packets addressed to the mobile node's IPv6 link-local address MUST NOT be tunneled to the mobile node. Instead, these packets MUST be discarded and the home agent SHOULD return an ICMPv6 Destination

Unreachable, Code 3, message to the packet's Source Address (unless this Source Address is a multicast address).

The home agent SHOULD check that all inner IPv6 packets received from the mobile node over a tunnel with outer source address the home address or the care-of 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 home addresses and/or prefixes the packet SHOULD be dropped.

Interception and tunneling IPv6 multicast addressed packets on the home network is only done if the home agent supports multicast group membership control messages from the mobile node as described in the next section. Multicast IPv6 packets addressed to a multicast address with link-local scope [RFC4291], to which the mobile node is subscribed, MUST NOT be tunneled to the mobile node. These packets SHOULD be silently discarded (after delivering to other local multicast recipients). Multicast packets addressed to a multicast address with a scope larger than link-local, but smaller than global (e.g., site- local and organization-local [RFC4291], to which the mobile node is subscribed, SHOULD NOT be tunneled to the mobile node. Multicast packets addressed with a global scope, to which the mobile node has successfully subscribed, MUST be tunneled to the mobile node.

4.3.3. IPv6 Multicast Membership Control

IPv6 multicast membership control is provided as defined in MIPv6 [RFC3775], Section 10.4.3. The only clarification required for the purpose of this specification is that all MLD [RFC2710] or MLDv2 [RFC3810] messages between the mobile node and the home agent MUST be tunneled between the mobile node and the home agent, bypassing the foreign agent.

4.4. Foreign Agent Considerations

A dual stack foreign agent that supports the IPv6 extensions defined in this specification MUST keep track of the following IPv6 related

state for the mobile IP clients it supports in addition to the state defined in [RFC3344].

- IPv6 Prefix(es) and Prefix Length(s)

- Tunneling mode for IPv6 traffic:

  - accept IPv6 encapsulated in IPv4 and reverse tunnel IPv6

  - IPv6 is tunneled directly to the IPv4 HoA so the foreign agent will not provide encapsulation/decapsulation services for IPv6 traffic for this mobile.

When a foreign agent receives a registration request with IPv6 Prefix Request extension(s) it has the following choices:

1) Ignore the extension(s). The registration request is forwarded as is to the home agent.

   The foreign agent SHOULD operate according to MIPv4 [RFC3344]

2) Attach an IPv6 tunneling mode extension to the registration request sent to the home agent.

   The foreign agent MUST be prepared to decapsulate and deliver IPv6 packets, in addition to the IPv4 packets, sent to it in the home agent to foreign agent tunnel for that mobile node. The foreign agent MUST be prepared to receive IPv6 packets from the mobile node, in addition to IPv4 packets. All IPv6 traffic MUST be reverse tunneled to the home agent by the foreign agent irrespectively from the reverse tunneling setting negotiated for IPv4 packets by mechanisms in [RFC3024]

If the foreign agent sets the R flag included in the mobility agent advertisement [RFC3344] and a mobile node uses the co-located address mode of operation, the foreign agent MUST NOT include an IPv6 tunneling mode extension in the registration request messages sent from that mobile node.

4.5. Mobile Node Considerations

A dual stack mobile node that supports the extensions described in this document MAY use these extensions to register its IPv6 home address(es) and/or 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 SHOULD 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].

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 SHOULD assume that these IPv6 prefixes are rejected.

For each matching IPv6 Prefix Reply extensions 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:

- If the care-of address mode of operation is used, the mobile node MUST be prepared to send/receive IPv6 traffic on its interface natively (i.e., without any Mobile IP related tunnel headers). If reverse tunneling is negotiated, then IPv6 traffic sent by the mobile node may be reverse tunneled via the foreign agent using either the direct delivery style or the encapsulating delivery style as defined in [RFC3024] for IPv4 traffic.

- If 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.

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 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 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 may not have appropriate state to process them.

4.6. Dynamic IPv6 Prefix allocation

The dynamic IPv6 prefix allocation described in the following section reuses the Mobile IPv4 mechanisms defined for IPv4 address allocation. An implementation can use a different mechanism to dynamically allocate IPv6 addresses in which case once such IPv6 addresses are allocated, they can be registered using the extensions and mechanism already described.

How a home agent decides to provide, or accept, an IPv6 home address or 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], or other mechanisms may be used to make such determination

4.6.1. Mobile IP Style Address Allocation

A mobile node may include one or more IPv6 Prefix Request extensions with the IPv6 prefix field set to zero. The mobile node MAY set the prefix length field of such extensions to zero or to a length of its choice as a hint to the home agent. Such IPv6 Prefix Request extensions indicate that the mobile node requests IPv6 address(es)

and prefix(es) to be assigned to it by the home agent.

A home agent receiving an IPv6 Prefix Request extension with the IPv6 prefix field set to zero MAY return an IPv6 Prefix Reply extension with the IPv6 prefix field set to the IPv6 prefix allocated to the mobile node. The length of that prefix is at the discretion of the home agent. The home agent may take into account the prefix length hint if one is included in the IPv6 Prefix Request extension.

A mobile node MAY include one or more IPv6 Prefix Request extensions with the IPv6 Prefix field set to ::interface_identifier, where interface_identifier is the unique layer 2 address of the client. The interface_identifier MUST be less than or equal to 64 bits in length. In this case the prefix length field MUST be set to 128.

The home agent MAY in this case return an IPv6 Prefix Reply extension with:

- the IPv6 prefix field set to PREFIX:: and the prefix length field set to the desired prefix length value. In this case the PREFIX:: subnet is allocated to the mobile node, which should proceed in constructing IPv6 addresses as defined in [RFC4862]

- the IPv6 prefix field set to PREFIX::interface_identifier and the prefix length field set to 128. In this case an individual IPv6 address is allocated to the mobile node.

4.7. Deregistration of IPv6 Prefix

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 address(es) and 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.

4.8. Registration with a private CoA

If the care-of address is a private address then Mobile IP NAT Traversal as [RFC3519] 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] MUST be set to the value for IPv6.

5. Security Considerations

This specification operates in the security constraints and requirements of [RFC3344]. It extends the operations defined in [RFC3344] for IPv4 home addresses to cover home IPv6 addresses prefixes and provides the same level of security for both IP address versions.

As defined in the security considerations section of RFC3344, ingress filtering in the data path may prevent mobiles from using triangular routing for their IPv6 communications even if the foreign agent used supports the dual stack extensions defined in this specification. In such cases reverse tunneling can be used to allow for effective ingress filtering in intermediate routers without blocking IPv6 traffic to reach its destination.

Home Agents MUST perform appropriate checks for reversed tunneled IPv6 packets similar to what is defined in [RFC3024] for IPv4 packets. The check defined in [RFC3024] 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 SHOULD check that the source address of the inner header is a register IPv4 or IPv6 home address 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.

6. IANA Considerations

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] at http://www.iana.org/assignments/mobileip-numbers.

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.

Finally, this specification creates a new space for the Code field of the IPv6 Prefix Reply extension. Values 0, 1, 8, 9, 10, 11 are defined in this specification. Values 0-7 are reserved for accept codes and the rest of the values are reserved for reject values.

Similar to the procedures specified for Mobile IPv4 [RFC3344] number spaces, future allocations from this number space require expert review [RFC2434].

7. Change history

NOTE TO RFC EDITOR: Remove Section 7 before publication.

7.1. Changes from v04 to v05

Corrected nits.

Added IANA considerations section.

7.2. Changes from v03 to v04

Clarified that DAD is only needed on IPv6 addresses and not prefixes, in Section 4.3.

Clarified of tunneling process in Section 4.3.2

Numerous editorial and clarification changes.

7.3. Changes from v02 to v03

Clarified high level description of implicit mode in Section 2.3 (thanks to Kent for suggesting appropriate text).

Clarified how IPv6 is tunneled over various tunneling modes allowed by MIPv4 in Section 4.3.2 (thanks to Alex for spotting this).

Numerous editorial and clarification changes.

7.4. Changes from v01 to v02

Expanded high level description of explicit mode in Section 2.3.

Fixed alignment of figures.

Fixed length fields in extensions to reflect short extension format correctly (thanks to Jun Awano for catching this one)

Removed section on Prefix Delegation and replaced it with more generic text that allows any other address allocation mechanism to be used to allocate IPv6 addresses and then extensions and mechanism described in this specification can be used to registered these addresses.

Numerous editorial and clarification changes.

7.5. Changes from v00 to v01

The Home Agent Considerations section was re-written and expanded with a lot more details by adapting text from MIPv6 and NEMO specifications.

New error codes were added to section 3.2

Allowed for any length prefix, not just 64 and 128.

Numerous editorial and clarification changes.

8. Acknowledgements

Thanks to Pat Calhoun, Paal Engelstad, Tom Hiller and Pete McCann for earlier work on this subject. Thanks also to Alex Petrescu for suggesting the use of additional mechanisms for dynamic IPv6 address allocation. Special thanks also to Sri Gundavelli and Kent Leung for their thorough review and suggestions.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3024] Montenegro, G., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[RFC3344] Perkins, C., "IP Mobility Support for IPv4", RFC 3344, August 2002.

[RFC3519] Levkowetz, H. and S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, May 2003.

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

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless

Address Autoconfiguration", RFC 4862, September 2007.

9.2. Informative References

[RFC2004] Perkins, C., "Minimal Encapsulation within IP", RFC 2004, October 1996.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

Authors' Addresses

George Tsirtsis
Qualcomm

Phone: +908-947-7059
Email: tsirtsis@qualcomm.com; tsirtsisg@yahoo.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

Full Copyright Statement

Intellectual Property

pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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