MEXT Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 1, 2008

R. Wakikawa (Ed.)
Toyota ITC/Keio Univ.
T. Ernst
INRIA
K. Nagami
INTEC NetCore
V. Devarapalli (Ed.)
Wichorus

April 30, 2008

Multiple Care-of Addresses Registration
draft-ietf-monami6-multiplecoa-07.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

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

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

This Internet-Draft will expire on November 1, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

According to the current Mobile IPv6 specification, a mobile node may have several care-of addresses, but only one, called the primary care-of address, that can be registered with its home agent and the correspondent nodes. However, for matters of cost, bandwidth, delay, etc, it is useful for the mobile node to get Internet access through multiple accesses simultaneously, in which case the mobile node would be configured with multiple active IPv6 care-of addresses. This document proposes extensions to the Mobile IPv6 protocol to register and use multiple care-of addresses. The extensions proposed in this document can be used by Mobile Routers using the NEMO (Network Mobility) Basic Support protocol as well.

Table of Contents

1. Introduction

A mobile node may use various types of network interfaces to obtain durable and wide area network connectivity. This is increasingly become true with mobile nodes having multiple interfaces such as 802.2, 802.11, 802.16, cellular radios, etc.. The motivations for and benefits of using multiple points of attachment are discussed in [ID-MOTIVATION]. When a mobile node with multiple interfaces uses Mobile IPv6 [RFC-3775] for mobility management, it cannot use its multiple interfaces to send and receive packets while taking advantage of session continuity provided by Mobile IPv6. This is because Mobile IPv6 allows the mobile node to only bind one care-of address at a time with its home address.

This document proposes extensions to Mobile IPv6 to allow a mobile node to register multiple care-of addresses for a home address and create multiple binding cache entries. A new Binding Identification (BID) number is created for each binding the mobile node wants to create and sent in the binding update. The home agent that receives this Binding Update creates separate binding for each BID. The BID information is stored in the corresponding binding cache entry. The BID information can now be used to identify individual bindings. The same extensions can also be used in Binding Updates sent to the correspondent nodes.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-2119].

Terms used in this draft are defined in [RFC-3775], [RFC-3753] and [RFC-4885]. In addition or in replacement of these, the following terms are defined or redefined:

Binding Identification number (BID)

The BID is an identification number used to distinguish multiple bindings registered by the mobile node. Assignment of distinct BIDs allows a mobile node to register multiple binding cache entries for a given home address. The BID MUST be unique for a binding to a specific care-of address for a given home address and care-of address pair. Zero and negative values MUST NOT be used. Each BID is generated and managed by a mobile node. The BID is stored in the Binding Update List and is sent by the mobile node in the Binding Update. A mobile node MAY change the value of a BID at any time according to its administrative policy, for instance to protect its privacy. An implementation must carefully assign the BID so as to keep using the same BID for the same binding even when the status of the binding is changed. More details can be found in Section 5.1.

Binding Identifier Mobility Option

The Binding Identifier mobility option is used to carry the BID information.

Bulk Registration

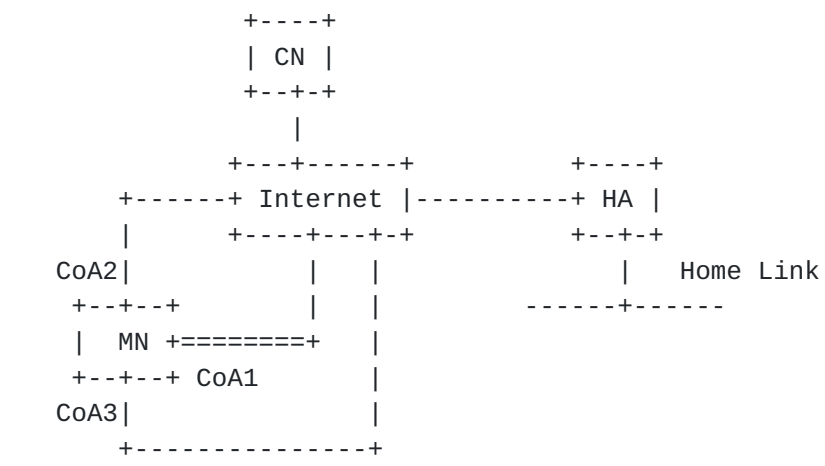
A mobile node can register multiple bindings at once by sending a single Binding Update. A mobile node can also replace some or all the bindings available at the home agent with the new bindings by using the bulk registration. Bulk registration is supported only for home registration (i.e. with the home agent) as explained in Section 5.4. A mobile node MUST NOT perform bulk registration with a correspondent node.

3. Protocol Overview

A new extension called the Binding identification number (BID) is introduced to distinguish between multiple bindings pertaining to the same home address. If a mobile node configures several IPv6 global addresses on one or more of its interfaces, it can register these addresses with its home agent as care-of addresses. If the mobile node wants to register multiple bindings, it MUST generate a BID for each care-of address and store the BID in the binding update list. A mobile node can manipulate each binding independently by using the BIDs. The mobile node then registers its care-of addresses by sending a Binding Update with a Binding Identifier mobility option. The BID is included in the Binding Identifier mobility option. After receiving the Binding Update with a Binding Identifier mobility option, the home agent MUST copy the BID from the Binding Identifier mobility option to the corresponding field in the binding cache entry. If there is an existing binding cache entry for the mobile node, and if the BID in the Binding Update does not match the one with the existing entry, the home agent MUST create a new binding cache entry for the new care-of address and BID. The mobile node can register multiple care-of addresses either independently in individual Binding Updates or multiple at once in a single Binding Update.

If the mobile host wishes to register its binding with a correspondent node, it must perform return routability operations. This includes managing a Care-of Keygen token per care-of address and exchanging CoTi and CoT message with the correspondent node for each care-of address. The mobile node MAY use the same BID that it used with the home agent for a particular care-of address. For protocol simplicity, bulk registration to correspondent nodes is not supported in this document. This is because the Return Routability mechanism introduced in [RFC-3775] cannot be easily extended to verify multiple care-of addresses stored in a single Binding Update.

Figure 1 illustrates the configuration where the mobile node obtains multiple care-of addresses at foreign links. The mobile node can utilize all the care-of address. In Figure 1, the home address of the mobile node (MN) is a:b:c:d::EUI. The mobile node has 3 different interfaces and possibly acquires care-of addresses 1-3 (CoA1, CoA2, CoA3). The mobile node assigns BID1, BID2 and BID3 to each care-of address.



Binding Cache Database:
home agent's binding (Proxy neighbor advertisement is active)
binding [a:b:c:d::EUI care-of address1 BID1]
binding [a:b:c:d::EUI care-of address2 BID2]
binding [a:b:c:d::EUI care-of address3 BID3]
correspondent node's binding
binding [a:b:c:d::EUI care-of address1 BID1]
binding [a:b:c:d::EUI care-of address2 BID2]
binding [a:b:c:d::EUI care-of address3 BID3]

Figure 1: Multiple Care-of Address Registration

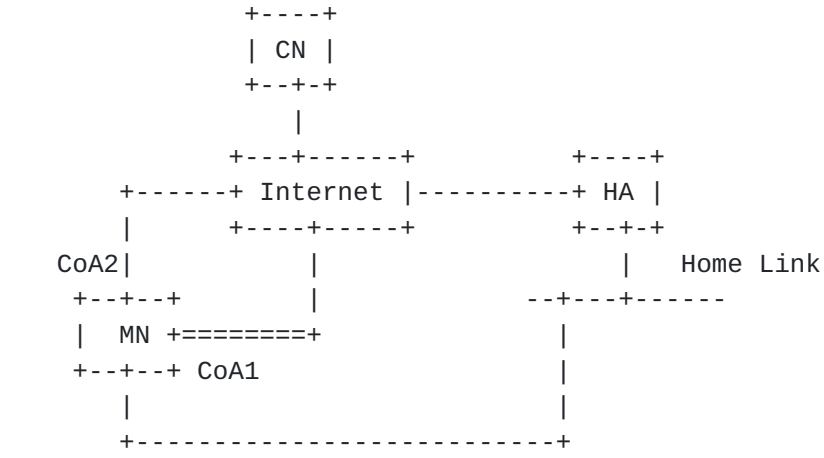
If the mobile node decides to act as a regular mobile node compliant with [RFC-3775], it sends a Binding Update without any Binding Identifier mobility options. The receiver of the Binding Update deletes all the bindings registering with a BID and registers only a single binding for the mobile node. Note that the mobile node can continue using the BID even if it has only a single binding that is active.

Binding cache lookup is done based on the home address and BID information. This is different from RFC 3775, where only the home address is used for binding cache lookup. The binding cache lookup may also involve policy or flow filters in cases where some policy or flow filters are used to direct certain packets or flows to a particular care-of address. The binding cache lookup using policy or flow filters is out of scope for this document. In case the binding cache lookup, using the combination of home address and BID, does not return a valid binding cache entry, the home agent MAY perform another lookup based on only the home address. This is implementation dependent and configurable on the home agent.

The mobile node may return to the home link through one of its interfaces. There are three options possible for the mobile node

when its returns home. Section 5.6 describes the returning home procedures in more detail.

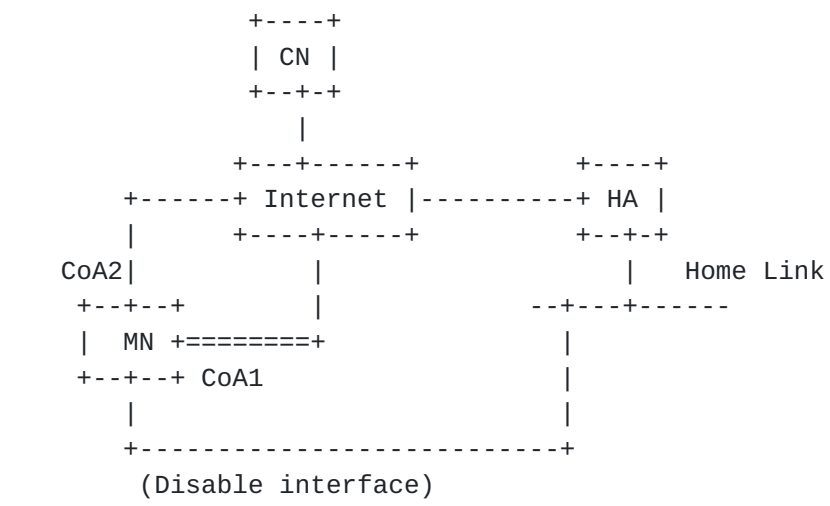
1. The mobile node uses only the interface with which it attaches to the home link. This is illustrated in Figure 2. It de-registers all bindings with the home agent related to all care-of addresses. The interfaces still attached to the visited link(s) are no longer going to be receiving any encapsulated traffic from the home agent. On the other hand, the mobile node can continue communicating with the correspondent node from the other interfaces attached to foreign links by using route optimization. Even if the mobile node is attached to the home link, it can still send Binding Updates for other active care-of addresses (CoA1 and CoA2) to correspondent nodes. Since the correspondent node has bindings, packets are routed to each Care-of Addresses directly.



Binding Cache Database:
home agent's binding
none
correspondent node's binding
binding [a:b:c:d::EUI care-of address1 BID1]
binding [a:b:c:d::EUI care-of address2 BID2]

Figure 2: Using only Interface Attached to Home Link

2. The mobile node uses only the interfaces still attached to the visited link(s) as shown in Figure 3. The interface with which the mobile node attaches to the home link is not used.

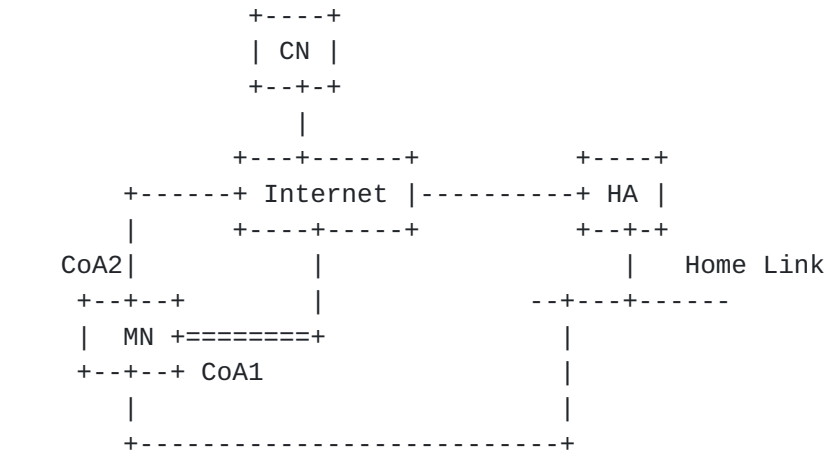



```
Binding Cache Database:
   home agent's binding
         binding [a:b:c:d::EUI  care-of address1  BID1]
         binding [a:b:c:d::EUI  care-of address2  BID2]
   correspondent node's binding
         binding [a:b:c:d::EUI  care-of address1  BID1]
         binding [a:b:c:d::EUI  care-of address2  BID2]
```

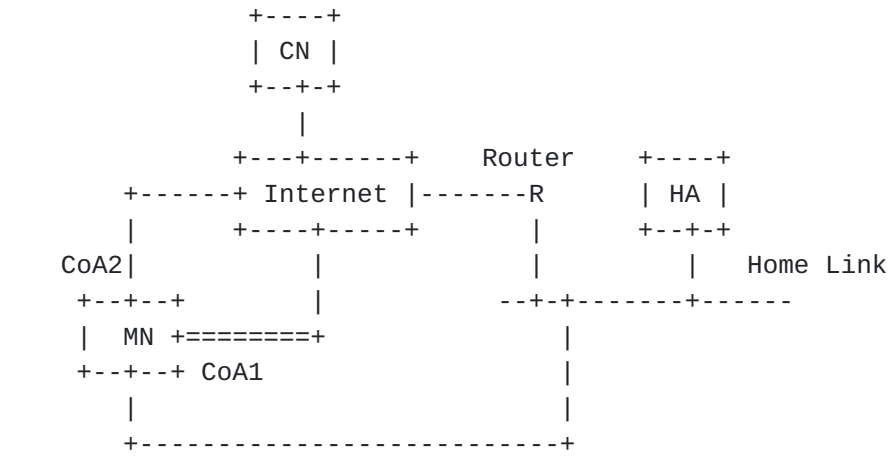
Figure 3: Using only interface attached to the visited link

3. The mobile node may simultaneously use both the interface attached to the home link and the interfaces still attached to the visited link(s) as shown in Figure 4. There are two possible topologies depending on whether the home agent is only router on the home link or not. The operation of Neighbor Discovery [RFC-2461] is different in the two topologies. The home agent and the correspondent node have the binding entries listed in Figure 4 in their binding cache database in both topologies. The home agent also knows that the mobile node has attached to the home link. All the traffic from the Internet is intercepted by the home agent first and routed to either the interface attached to the home link or the one of the foreign links. How the home agent decides to route a particular flow to the interface attached to the home link or foreign link is out of scope in this document.

Topology-a)



Topology-b)



Binding Cache Database:

home agent's binding

binding [a:b:c:d::EUI care-of address1 BID1]

binding [a:b:c:d::EUI care-of address2 BID2]

correspondent node's binding

binding [a:b:c:d::EUI care-of address1 BID1]

binding [a:b:c:d::EUI care-of address2 BID2]

Figure 4: Simultaneous Home and Visited Link Operation

4. Mobile IPv6 Extensions

This section summarizes the extensions to Mobile IPv6 necessary for manage multiple bindings.

4.1. Binding Cache Structure and Binding Update List

The BID is required to be stored in the binding cache and binding update list structure.

The sequence number value SHOULD be shared among all the binding update list entries related to binding updates sent to a particular home agent or correspondent node. Whenever a mobile node sends either individual or bulk binding update, the sequence number is incremented. On the other hand, if a mobile node manages an individual sequence value per binding update list, a mobile node SHOULD carefully select the sequence number value for the bulk binding update. This is because all the bulk-registered bindings use the same Sequence Number specified in the Binding Update. If each binding uses different sequence number, a mobile node MUST use the largest sequence number from the Binding Update list entries used for the bulk registration. If the mobile node cannot select a sequence number for all the bindings due to sequence number out of window, it MUST NOT use the bulk registration for the binding whose sequence number is out of window. A separate Binding Update should be sent for the binding.

4.2. Binding Identifier Mobility Option

The Binding Identifier mobility option is included in the Binding Update, Binding Acknowledgement, Binding Refresh Request, and Care-of Test Init and Care-of Test message.

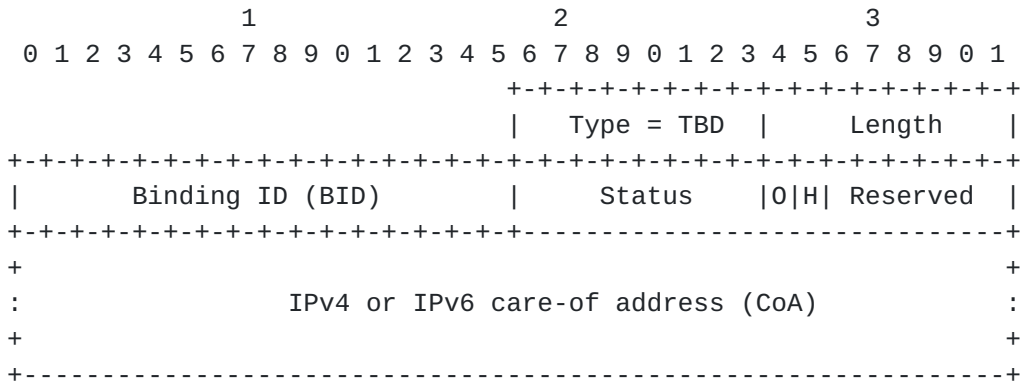


Figure 5: BID Mobility Option

Type

Type value for Binding Identifier is TBD

Length

8-bit unsigned integer. Length of the option, in octets, excluding the Type and Length fields. It MUST be set to either 4, 12, or 20 depending on the care-of address field. When the care-of address is not carried by this option, the length value MUST be set to 4. If the IPv4 care-of address is stored in the care-of address field, the length MUST be 12. Otherwise, the Length value MUST be set to 20 for IPv6 care-of address.

Binding ID (BID)

The BID which is assigned to the binding indicated by the care-of address in the Binding Update or the BID mobility option. The BID is a 16-bit unsigned integer. The value of zero is reserved and MUST NOT be used.

Status

When the Binding Identifier mobility option is included in a Binding Acknowledgement, this field overwrites the status field in the Binding Acknowledgement. If this field is zero, the receiver MUST use the registration status stored in the Binding Acknowledgement message. This Status field is also used to carry error information related to the care-of address test in the Care-of Test message. The status is 8-bit unsigned integer. The possible status codes are the same as the status codes of Binding Acknowledgement.

Overwrite (O) flag

When this flag is set, a mobile node requests the recipient to replace all the bindings to binding entries stored in a Binding Update.

Simultaneous Home and Foreign Binding (H) flag

This flag indicates that the mobile node registers multiple bindings to the home agent while is attached to the home link. This flag is valid only for a Binding Update sent to the home agent.

Reserved

5 bits Reserved field. The reserved field MUST be zero.

Care-of Address

This field has the variable length depending on the specified flags. Either IPv4 or IPv6 care-of address for the corresponding BID can be stored in this field. This field MUST NOT be used if a Binding Identifier mobility option is included in any other message other than a Binding Update.

4.3. New Status Values for Binding Acknowledgement

New status values for the status field in a Binding Acknowledgement are defined for handling the multiple Care-of Addresses registration:

MCOA NOTCOMPLETE (TBD < 128)

In bulk registration, not all the binding identifier mobility option are successfully registered. Some of them are rejected. The error status value of the failed mobility option is individually stored in the status field of the binding identifier mobility option.

MCOA RETURNHOME WO/NDP (TBD < 128)

When a mobile node returns home, it MUST NOT use NDP for the home address on the home link. This is explained in more detail in Section 5.6

MCOA MALFORMED (TBD more than 128)

Registration failed because Binding Identifier mobility option was not formatted correctly.

MCOA BID CONFLICT (TBD more than 128)

The home agent cannot cache both a regular binding and a BID extended binding simultaneously. It returns this status value when the received binding conflicts with the existing binding cache entry(ies).

MCOA PROHIBITED(TBD more than 128)

It implies the multiple care-of address registration is administratively prohibited.

MCOA BULK REGISTRATION NOT SUPPORTED (TBD more than 128)

Bulk binding registration is not supported.

5. Mobile Node Operation

5.1. Management of Care-of Address(es) and Binding Identifier(s)

There are two cases when a mobile node might acquire several care-of addresses. Note that a mixture of the two cases is also possible.

1. A mobile node may be using several physical network interfaces and acquires a care-of address on each of its interfaces.

2. A mobile node uses a single physical network interface, but receives advertisements for multiple prefixes on the link the interface is attached to. This will result in the mobile node configuring several global addresses on the interface from each of the announced prefixes.

The difference between the above two cases is only in the number of physical network interfaces and therefore irrelevant in this document. What is of significance is the fact that the mobile node has several addresses it can use as care-of addresses.

A mobile node assigns a BID to each care-of address when it wants to register them simultaneously with its home address. The BID MUST be unique for a given home address and care-of address pair. The value should be an integer between 1 and 65535. Zero and negative values MUST NOT be used as BIDs. If a mobile node has only one care-of address, the assignment of a BID is not needed until it has multiple care-of addresses to register with, at which time all of the care-of addresses MUST be mapped to BIDs.

5.2. Return Routability: Sending CoTI and Receiving CoT

When a mobile node wants to register multiple care-of address with a correspondent node, it MUST have the valid Care-of Keygen token per care-of address. The mobile node needs only one Home Keygen token for its home address.

The mobile node MUST include a Binding Identifier mobility option in the Care-of Test Init message. It MUST NOT set any flags in the mobility option. The receiver (i.e. correspondent node) will calculate a care-of Keygen token as specified in [RFC-3775] and reply with a Care-of Test message, with the Binding Identifier mobility option as described in Section 6.2. When the mobile node receives the Care-of Test message, the message is verified as in [RFC-3775]. If a Binding Identifier mobility option is not present in the CoT message in reply to the CoTI message that included a Binding Identifier mobility option, the mobile node must assume that the correspondent node does not support Multiple Care-of Address

registration. Thus, the mobile node MUST NOT use a Binding Identifier mobility option in any future Binding Updates to that correspondent node. The mobile node MAY skip re-sending regular CoTI message and keep the received care-of Keygen token for the regular Binding Update.

5.3. Binding Registration

For the multiple Care-of Addresses registration, the mobile node MUST include a Binding Identifier mobility option(s) in the Binding Update as shown in Figure 6. The BID is copied from a corresponding Binding Update List entry to the BID field of the Binding Identifier mobility option. When IPsec ESP is used for protecting the Binding Update, the care-of address can be carried in the Care-of Address field of the Binding Identifier mobility option. If this is done, the alternate care-of address option MUST NOT be included in the Binding Update. For binding registration to a correspondent node, the mobile node MUST have both active Home and Care-of Keygen tokens for Kbm (see Section 5.2.5 of [RFC-3775]) before sending the Binding Update. The care-of Keygen tokens MUST be maintained for each care-of address that the mobile node wants to register to the correspondent node. The Binding Update to the correspondent node is protected by the Binding Authorization Data mobility option that is placed after the Binding Identifier mobility option.

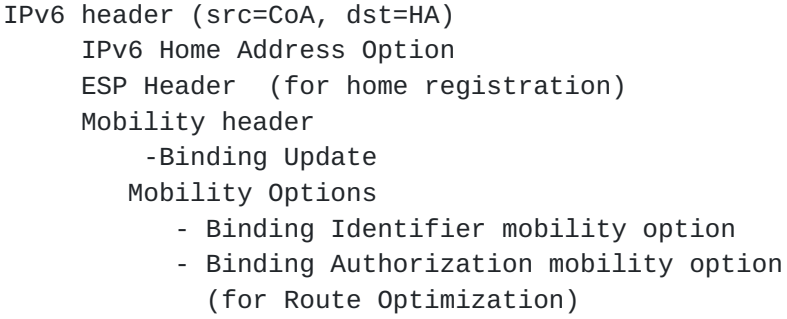


Figure 6: Binding Update for Binding Registration

5.4. Bulk Registration

Bulk registration is an optimization for binding multiple care-of addresses to a home address using a single Binding Update. This is very useful if the mobile node, for instance, does not want to send a lot of signaling messages through an interface where the bandwidth is scarce. This document specifies bulk registration only for the mobile node's home registration. A mobile node performing bulk registration with a correspondent node is out of scope.

To use bulk registration, the mobile node includes a Binding

Identifier Mobility option for each BID and Care-of address pair it wants to register in the same Binding Update message. This is shown in Figure 7. The rest of the fields and options in the Binding Update such as Lifetime, Sequence Number, and the flags in the Binding Update are common across all care-of addresses. The alternate care-of address option MUST NOT be used.

```
IPv6 header (src=CoA, dst=HA)
     IPv6 Home Address Option
     ESP Header
     Mobility header
         -Binding Update
        Mobility Options
           - Binding Identifier mobility options (CoA)
```

Figure 7: Binding Update for Bulk Registration

If the mobile node wants to replace existing registered bindings on the home agent with the bindings in the sent Binding Update, it sets the 'O' flag. Section 6.3 describes this registration procedure in detail.

5.5. Binding De-Registration

When a mobile node decides to delete all the bindings for its home address, it sends a regular de-registration Binding Update with lifetime set to zero as defined in [RFC-3775]. The Binding Identifier mobility option is not required.

If a mobile node wants to delete a particular binding(s) from its home agent and correspondent nodes, the mobile node sends a Binding Update with lifetime set to zero and includes a Binding Identifier mobility option(s) with the BID(s) it wants to de-register. The receiver will remove only the care-of address(es) that match(es) the specified BID(s). The care-of addresses field in each mobility option SHOULD be omitted by the sender and MUST be ignored by the receiver. This is because the receiver will remove the binding that matches the specified BID.

5.6. Returning Home

The mobile node may return to the home link, by attaching to the home link through one of its interfaces. When the mobile node wants to return home, it should be configured with information on what interface it needs to use. The mobile node may use only the interface with which it is attached to the home link, only the interfaces still attached to the visited link(s) or use both interfaces attached to the home link and visited link(s)

simultaneously. The following describes each option in more detail.

5.6.1. Using only Interface attached to the Home Link

The mobile node returns home and de-registers all the bindings as shown in Figure 2 and as defined in [RFC-3775]. De-registering all the bindings is the same as binding de-registration from foreign link described in Section 5.5. After the de-registration step, all the packets routed by the home agent are only forwarded to the interface attached to the home link, even if there are other active interfaces attached to the visited link(s). While the mobile node de-registers all the bindings from the home agent, it may continue registering bindings for interface(s) attached to visited link(s) to the correspondent node as shown in Figure 2.

5.6.2. Using only Interface attached to the Visited Link

The mobile node returns home and shuts down the interface attached to the home link as shown in Figure 3. Before shutting down the interface, any binding for the care-of address previously associated with the interface should be deleted. To delete the binding cache entry, the mobile node SHOULD send a de-registration Binding Update with the lifetime set to zero and include the corresponding BID information. If the mobile node does not send a de-registration Binding Update, the binding for the care-of address previously assigned to the interface remains at the home agent until its lifetime expires.

In this scenario, despite the fact that the mobile node is connected to its home link, all of its traffic is sent and received via the home agent and its foreign links.

5.6.3. Simultaneous Home and Visited Link Operation

[Problems of Simultaneous Home and Foreign Attachments]

The mobile node returns home and continues using all the interfaces attached to both foreign and home links as shown in Figure 4. The mobile node indicates this by setting the 'H' flag in the BID mobility option as defined below. There are additional requirements on the Returning Home procedures for possible Neighbor Discovery states conflicts at the home link.

In [RFC-3775], the home agent intercepts packets meant for the mobile node using the Proxy Neighbor Discovery [RFC-2461] while the mobile node is away from the home link. When the mobile node returns home, the home agent deletes the binding cache and stops proxying for the

home address so that a mobile node can configure its home address on the interface attached to the home link. In this specification, a mobile node may return home, configure the home address on the interface attached to the home link, but still use the interfaces attached to the foreign links. In this case, a possible conflict arises when the both the home agent and the mobile node try to defend the home address. If the home agent stops proxying for the home address, the packets are always routed to the interface attached to the home link and are never routed to the interfaces attached to the visited links. It is required to avoid the conflict between the home agent and the mobile node, while still allowing the simultaneous use of home and foreign links. The following describes the mechanism for achieving this.

[Overview and Approach]

In this specification, the home agent MUST intercept all the packets meant for the mobile node and decide whether to send the traffic directly to the home address on the link or tunnel to the care-of address. The home agent intercepts all the packets even when the mobile node is attached to the home link through one of its interfaces. The home agent would make this decision based on the type of flow. How to make this decision is out of scope in this document.

Two scenarios are illustrated in Figure 4, depending on whether the Home Agent is the only router at the home link or not. The difference is on who defends the home address by (Proxy) Neighbor Discovery on the home link.

1. Mobile node defends the home address by the regular Neighbor Discovery Protocol (illustrated as topology-a in Figure 4). The home agent is the only router on the home link. Therefore the home agent is capable of intercepting packets without relying on the proxy Neighbor Discovery protocol and the mobile node can manage the Neighbor Cache entry of the home address on the home link as a regular IPv6 node.

2. If there are other routers on the home link apart from the home agent, then it cannot be guaranteed that all packets meant for the mobile node are routed to the home agent. In this case, the mobile node MUST NOT operate Neighbor Discovery protocol for the home address on the home link. This allows the home agent to keep using proxy neighbor discovery and thus it keeps receiving all the packets sent to the mobile node's home address. If the home agent, according to its local policy, needs to deliver packets to the mobile node over the home link, an issue arises

with respect to how the home agent discovers the mobile node's link local address. This specification uses Link-layer Address (LLA) Option defined in [RFC-4068bis] in order to carry the mobile node's link-layer address in the Binding Update. Likewise, the mobile node would also know the link-layer address of the default router address to send packets from the home link without Neighbor Discovery. The link-layer address is used to transmit packets from and to the mobile node on the home link. The packets are transmitted without the Neighbor Discovery protocol by constructing the link-layer header manually. This operation is similar to Mobile IPv6 [RFC-3775] when a mobile node sends a deregistration binding update to the home agent's link-layer address in returning home operation.

[Sending Deregistration Binding Update]

- As soon as a mobile node returns home, it sends a de-registration Binding Update to the home agent from the interface attached to the home link.

- The mobile node MUST include the BID mobility option specifying the BID the mobile node had previously associated with the interface attached to the home link. The 'H' flag MUST be set in the BID mobility option. Any address MUST NOT be set in the Care-of Address field in the BID mobility option. When the 'H' flag is set, the home agent recognizes that the mobile node wants to continue using interfaces attached to both home and visited links. Note that H flag MUST be set for all the binding updates sent from the mobile node (ex. Binding Update for the interface(s) attached to the foreign link(s)).

- The mobile node SHOULD include the Link-layer Address (LLA) Option [RFC-4068bis] to notify the mobile node's link-layer address to the home agent, too. The option code of the Link-layer Address (LLA) option MUST be set to '2' (Link-layer Address of the mobile node). This link-layer address is required for the home agent to send the Binding Acknowledgement and to forward the mobile node's packet.

- According to [RFC-3775], the mobile node MUST start responding to Neighbor Solicitation for its home address right after it sends the deregistration Binding Update to the home agent. However, in this specification, the mobile node MUST NOT respond to Neighbor Solicitation before receiving a Binding Acknowledgement, since the home agent may continue proxying for the home address. If the mobile node receives [MCOA RETURNHOME WO/NDP (TBD)] status value in the received Binding Acknowledgment, it MUST NOT respond to

Neighbor Solicitation even after the Binding Acknowledgement.

[Sending Binding Acknowledgement]

- When the home agent sends the Binding Acknowledgement after successfully processing the binding de-registration, it MUST set the status value to either 0 [Binding Update Accepted] or to [MCOA RETURNHOME WO/NDP (TBD)] in the Status field of the Binding Acknowledgment depending on home agent configuration at the home link. The new values are:

  * Binding Update Accepted (0): NDP is permitted for the home address at the home link. This is regular returning home operation of [RFC-3775]

  * MCOA RETURNHOME WO/NDP (TBD): NDP is prohibited for the home address at the home link

  If the binding update is rejected, the appropriate error value MUST be set to the status field. In this case, the home agent operation is same as [RFC-3775].

- If the home agent is the only router at the home link, it stops proxy Neighbor Discover for the requested home address and responds with the [Binding Update Accepted] status value to the mobile node. Since the mobile node will not reply to Neighbor Solicitation for the home address before receiving the Binding Acknowledgement, the home agent SHOULD use the link-layer address carried by the Link Layer Address option [RFC-4068bis] in the received Binding Update. After the completion of the binding deregistration, the mobile node starts regular Neighbor Discovery operations for the home address on the home link. The neighbor cache entry for the home address is created by the regular exchange of Neighbor Solicitation and Neighbor Advertisement.

- On the other hand, if the home agent is not the only router on the home link, it returns [MCOA RETURNHOME WO/NDP] value in the Status field of the BID mobility option. The home agent learns the mobile node's link-layer address by receiving the link-layer address option carried by the Binding Update. It stores the link-layer address as a neighbor cache entry for the mobile node so that it can send the packets to the mobile node's link-layer address.

- Note that the use of proxy Neighbor Discovery is easier way to intercept the mobile nodes' packets instead of IP routing in some deployment scenarios. Therefore, even if a home agent is the only

router, it is an implementation and operational choice whether the home agent returns [Binding Update Accepted] or [MCOA RETURNHOME WO/NDP].

- If BID option is not included in the Binding Acknowledgement, the home agent might not recognize the simultaneous home and foreign attachment. The home agent might have processed the de-registration Binding Update as a regular de-registration as described in [RFC-3775] and deletes all the registered binding cache entries for the mobile node. Thus, the mobile node SHOULD stop using the interface attached to foreign link and use only the interface attached to the home link.

[Sending Packets from the Home Link]

- When the mobile node receives the Binding Acknowledgement with the status value 'Binding Update Accepted' and the BID option, it can configure its home address to the interface attached to the home link and start operating Neighbor Discovery for the home address on the home link. Packets can be transmitted from and to the mobile node as if the mobile node is a regular IPv6 node.

- If the mobile node receives the status [MCOA RETURNHOME WO/NDP] in the Binding Acknowledgement, it MUST NOT operate Neighbor Discovery for the home address. When the mobile node sends packets from the interface attached to the home link, it MUST learn the link-layer address of the next hop (i.e. default router of the mobile node). A mobile node learns the default router's link-layer address from a Source Link-Layer Address option in Router Advertisements. The mobile node sends packets directly to the default router's link-layer address. This is done by constructing the packet including link-layer header with the learned link-layer address of the default router. The home agent also forwards the packet to the mobile node on the home link by using the mobile node's link-layer address. The link-layer address SHOULD be cached when the home agent received the deregistration Binding Update message.

[Leaving from the Home Link]

- When the mobile node detaches from the home link, it SHOULD immediately send a binding update for one of active care-of address with H flag unset. When the 'H' flag of BID option is unset in any Binding Update, the home agent stop forwarding the mobile node's packet to the home link.

- On the other hand, if the mobile node does not have any active care-of address to send a Binding Update and leaves the home link (i.e. the mobile node is completely disconnected), the home agent continues forwarding packets to the mobile node until the expiration of all the binding cache entries for the home address. Once all the bindings are expired, the mobile node is assumed to be disconnected completely from networks.

[Changing Behavior during the attachment to the home link]

If a mobile node decides to return home completely without any active foreign link attachment, it simply sends a deregistration binding update as described in Section 5.6.1. Once the home agent receives such de-registration binding update, the home agent clears all the binding and states for the mobile node.

If a mobile node decides to stop using the interface attached to the home link, it simply sends a binding update from the one of active care-of address. In the Binding Update, the mobile node should include the BID option for the care-of address and unset the H flag of BID option. The home agent clears the states of the mobile node for the interface attached to the home link and stop forwarding the packets to the mobile node on the home link.

5.7. Receiving Binding Acknowledgement

The verification of a Binding Acknowledgement is the same as Mobile IPv6 (section 11.7.3 of [RFC-3775]). The operation for sending a Binding Acknowledgement is described in Section 6.3.

If a mobile node includes a Binding Identifier mobility option in a Binding Update with the 'A' flag set, a Binding Acknowledgement MUST carry a Binding Identifier mobility option. If no such mobility option is included in the Binding Acknowledgement in response to a Binding Update for multiple care-of address registration, this indicates that the originating node of the Binding Acknowledgement does not support processing the Binding Identifier mobility option. The mobile node MUST then stop multiple care-of address registration with that node.

If a Binding Identifier mobility option is present in the received Binding Acknowledgement, the mobile node checks the status field in the option. If the status value in the Binding Identifier mobility option is zero, the mobile node uses the value in the Status field of the Binding Acknowledgement. Otherwise, it uses the value in the Status field of the Binding Identifier mobility option.

If the status code is greater than or equal to 128, the mobile node starts relevant operations according to the error code. Otherwise, the mobile node assumes that the originator (home agent or correspondent node) successfully registered the binding information and BID for the mobile node.

- If the Status value is [MCOA PROHIBITED], the mobile node MUST stop registering multiple bindings to the node that sent the Binding Acknowledgement.

- If the Status value is [MCOA BULK REGISTRATION NOT SUPPORT], the mobile node SHOULD stop using bulk registrations with the node that sent the Binding Acknowledgement.

- If [MCOA MALFORMED] is specified, it indicates that the binding identifier mobility option is formatted wrongly.

- If [MCOA BID CONFLICT] is specified, the binding entry specified by the Binding Identifier mobility option is already registered as a regular binding. In such case, the mobile node SHOULD stop sending Binding Updates with BID, or SHOULD use the 'O' flag to reset all the registered bindings.

5.8. Receiving Binding Refresh Request

The verification of a Binding Refresh Request is the same as in Mobile IPv6 (section 11.7.4 of [RFC-3775]). The operation of sending a Binding Refresh Request is described in section Section 6.4.

If a mobile node receives a Binding Refresh Request with a Binding Identifier mobility option, it indicates that the node sending the Binding Refresh Request message is requesting the mobile node to send a new Binding Update for the BID. The mobile node SHOULD then send a Binding Update only for the respective binding. The mobile node MUST include a Binding Identifier mobility option in the Binding Update.

5.9. Bootstrapping

When a mobile node bootstraps and registers multiple bindings for the first time, it MUST set the 'O' flag in the Binding Identifier mobility option. If old bindings still exists at the home agent, the mobile node has no knowledge of which bindings still exist at the home agent. This scenario happens when a mobile node reboots and looses state regarding the registrations. If the 'O' flag is set, all the bindings are replaced by the new binding(s). If the mobile node receives the Binding Acknowledgement with the status code set to 135 [Sequence number out of window], it MUST retry sending a Binding Update with the last accepted sequence number indicated in the

Binding Acknowledgement.

The 'O' flag can also be used in individual Binding Updates sent to the correspondent nodes to override any existing binding cache entries at the correspondent node.

6. Home Agent and Correspondent Node Operation

6.1. Searching Binding Cache with Binding Identifier

If either a correspondent node or a home agent has multiple bindings for a mobile node in their binding cache database, it can use any of the bindings to communicate with the mobile node. This section explains how to retrieve the desired binding for the binding management. This document does not provide any mechanism to select the suitable binding for forwarding data packets.

A correspondent node SHOULD use both the home address and the BID as the search key of the binding cache if it knows the corresponding BID (ex. when processing signaling messages). In the example below, if a correspondent node searches the binding with the home address and BID2, it gets binding2 for this mobile node.

```
binding1 [a:b:c:d::EUI,  care-of address1,  BID1]
binding2 [a:b:c:d::EUI,  care-of address2,  BID2]
binding3 [a:b:c:d::EUI,  care-of address3,  BID3]
```

Figure 8: Searching the Binding Cache

A correspondent node learns the BID when it receives a Binding Identifier mobility option. At that time, the correspondent node MUST look up its binding cache database with the home address and the BID retrieved from the Binding Update. If the correspondent node does not know the BID, it searches for a binding with only the home address. In such a case, the first matched binding is found. If the correspondent node does not desire to use multiple bindings for a mobile node, it can simply ignore the BID.

6.2. Receiving CoTI and Sending CoT

When a correspondent node receives a CoTI message which contains a Binding Identifier mobility option, it processes it as follows.

First, the CoTI message is verified as specified in [RFC-3775]. The Binding Identifier mobility option is processed as follows:

- If a correspondent node does not understand a Binding Identifier mobility option, it just ignores and skips processing the option. The calculation of a care-of Keygen token will thus be done without a BID value. The correspondent node returns a CoT message without a Binding Identifier mobility option. The mobile node knows whether the correspondent supports processing the Binding Identifier mobility option, by checking if the option is present in the CoT message.

- If either the 'C' or the 'O' flag is set in the Binding Identifier mobility option, the correspondent Node SHOULD NOT calculate a care-of Keygen token, but MUST include a Binding Identifier mobility option with status value set to [MCOA MALFORMED] in the Care-of Test message.

- Otherwise, the correspondent node MUST include a Binding Identifier mobility option with status value set to zero (success) in the Care-of Test message.

- The Care-of address field of each Binding Identifier mobility option, can be omitted, because the mobile node can identify the corresponding Binding Update list entry using the BID.

6.3. Processing Binding Update

If a Binding Update does not contain a Binding Identifier mobility option, its processing is same as in [RFC-3775]. If the receiver already has multiple bindings for the home address, it MUST replace all the existing bindings by the received binding. As a result, the receiver node MUST have only one binding cache entry for the mobile node. If the Binding Update is for de-registration, the receiver MUST delete all existing bindings from its Binding Cache.

If the Binding Update contains a Binding Identifier mobility option(s), it is first validated according to section 9.5.1 of [RFC-3775]. Then the receiver processes the Binding Identifier mobility option(s) as described in the following steps.

- The length value is examined. The length value MUST be either 4, 8, or 20 depending on the Care-of Address field. If the length is incorrect, the receiver MUST reject the Binding Update and returns the status value set to [MCOA MALFORMED].

- When the Length value is either 12 or 20, the care-of address MUST be present in the Binding Identifier mobility option. If the care-of address is not present, the receiver MUST reject the Binding Identifier mobility option and returns the status value set to [MCOA MALFORMED]. If the Length value is 12, an IPv4 valid address MUST be present. Otherwise, an IPv6 address MUST be stored in the Binding Identifier mobility option.

- When multiple Binding Identifier mobility options are present in the Binding Update, it is treated as bulk registration. If the receiving node is a correspondent node, it MUST reject the Binding Update and returns the status value in the binding acknowledgement set to [MCOA BULK REGISTRATION NOT SUPPORT]

- If the Lifetime field in the Binding Update is set to zero, the receiving node deletes the binding entry that corresponds to the BID in the Binding Identifier mobility option. If the receiving node does not have an appropriate binding for the BID, it MUST reject the Binding Update and send a Binding Acknowledgement with status set to 133 [not home agent for this mobile node].

- If the 'O' flag is set in the de-registering Binding Update, it is ignored. If the 'H' flag is set, the home agent stores a home address in the Care-of Address field of the binding cache entry. The home agent also stops performing proxy ND for the mobile node's home address.

- If the Lifetime field is not set to zero, the receiving node registers a binding with the specified BID as a mobile node's binding. The Care-of address is obtained from the Binding Update packet as follows:

  * If the Length value of the Binding Identifier mobility option is 20, the care-of address is copied the IPv6 address from the care-of address field in the Binding Identifier mobility option. When the Length value is 12, the address MUST be the IPv4 valid address. Detail information can be found in Section 8.

  * If the Length value of the Binding Identifier mobility option is 4, the care-of address is copied from the source address field of the IPv6 header.

  * If the Length value of the Binding Identifier mobility option is 4 and an alternate care-of address is present, the care-of address is copied from the Alternate Care-of address mobility option.

- Once the care-of address(es) have been retrieved from the Binding Update, the receiving nodes creates new binding(s).

  * If only the 'O' flag is set in the Binding Identifier mobility option, the home agent removes all the existing bindings and registers the received bindings.

  * If the receiver has a regular binding which does not have BID for the mobile node, it must not process the binding update. The receiver should sent a binding acknowledgement with status set to [MCOA BID CONFLICT].

  * If the receiver already has a binding with the same BID but different care-of address, it MUST update the binding and

respond with a Binding Acknowledgement with status set to 0 [Binding Update accepted].

* If the receiver does not have a binding entry for the BID, it registers a new binding for the BID and responds with a Binding Acknowledgement with status set to 0 [Binding Update accepted].

If all the above operations are successfully completed, a Binding Acknowledgement containing the Binding Identifier mobility options MUST be sent to the mobile node. Whenever a Binding Acknowledgement is sent, all the Binding Identifier mobility options stored in the Binding Update MUST be copied to the Binding Acknowledgement except the status field. The Care-of address field in each Binding Identifier mobility option, however, can be omitted, because the mobile node can match a corresponding binding update list entry using the BID.

When a correspondent node sends a Binding Acknowledgement, the status value MUST be always stored in the Status field of the Binding Acknowledgement and the Status field of Binding Identifier mobility option set to zero. For the home agent, the status value can be stored in the Status field of either a Binding Acknowledgement or a Binding Identifier mobility option. If the status value is specific to one of bindings in the bulk registration, the status value MUST be stored in the Status field in the corresponding Binding Identifier mobility option. In this case, [MCOA NOTCOMPLETE] MUST be set to the Status field of the Binding Acknowledgement so that the receiver can examine the Status field of each Binding Identifier mobility option for further operations.

6.4. Sending Binding Refresh Request

When a node (home agent or correspondent node) sends a Binding Refresh Request for a particular binding created with the BID, the node SHOULD include the Binding Identifier mobility option in the Binding Refresh Request. If the mobile node had used bulk registration, the sender SHOULD include all the Binding Identifier mobility options. If the mobile node had not used bulk registration, the sender includes the Binding Identifier mobility options only for those bindings that need to be refreshed.

6.5. Receiving Packets from Mobile Node

When a node receives packets with a Home Address destination option from a mobile node, it MUST check that the care-of address that appears in the source address field of the IPv6 header MUST be equal to one of the care-of addresses in the binding cache entry. If no binding is found, the packets MUST be silently discarded. The node

MUST also send a Binding Error message as specified in [RFC-3775].
This verification MUST NOT be done for a Binding Update.

7. Network Mobility Applicability

The binding management mechanisms are the same for a mobile host that uses Mobile IPv6 and for a mobile router that is using the NEMO Basic Support protocol [RFC-3963]. Therefore the extensions described in this document can also be used to support a mobile router with multiple care-of addresses.

8. DSMIPv6 Applicability

Dual Stack Mobile IPv6 (DSMIPv6) [ID-DSMIPv6] extends Mobile IPv6 to register an IPv4 care-of address instead of the IPv6 care-of address when the mobile node is attached to an IPv4-only access network. It also allows the mobile node to acquire an IPv4 home address in addition to an IPv6 home address for use with IPv4-only correspondent nodes. This section describes how multiple care-of address registration works with IPv4 care-of and home addresses.

8.1. IPv4 Care-of Address Registration

The mobile node can use the extensions described in the document to register multiple care-of addresses, even if some of the care-of addresses are IPv4 address.

Bulk registration MUST NOT be used for the initial binding from an IPv4 care-of address. This is because, the Binding Update and binding acknowledgement exchange is used to detect NAT on the path between the mobile node and the home agent. So the mobile node needs to check for a NAT between each IPv4 care-of address and the home agent.

The Binding Update MUST be sent to the IPv4 home agent address by using UDP and IPv4 headers as shown in Figure 9. It is similar to [ID-DSMIPv6] except that the IPv4 care-of address option MUST NOT be used when the BID mobility option is used.

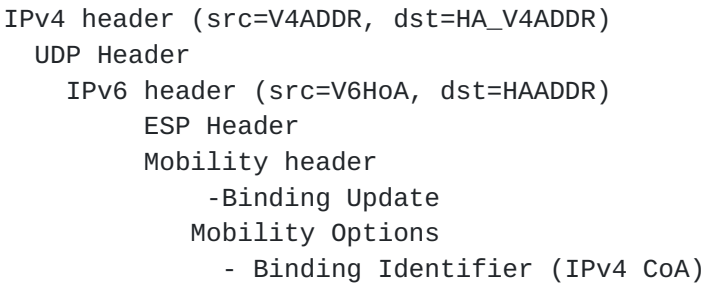


Figure 9: Initial Binding Update for IPv4 Care-of Address

If a NAT is not detected, the mobile node can update the IPv4 care-of address by using bulk registration. The mobile node can register the IPv4 care-of address along with other IPv4 and IPv6 care-of addresses. Figure 10 shows the Binding Update format when the mobile node sends a Binding Update from one of its IPv6 care-of addresses. If the mobile node sends a Binding Update from IPv4 care-of address, it MUST follow the format described in Figure 9. Note that the IPv4 Care-of Address must be registered by non bulk Binding registration, whenever it is changed.

```
IPv6 header (src=V6CoA, dst=HAADDR)
      IPv6 Home Address Option
      ESP Header
      Mobility header
          -Binding Update
         Mobility Options
            - Binding Identifier (IPv6/v4 CoA)
            - Binding Identifier (IPv6/v4 CoA)
            - ...
```

Figure 10: Binding Bulk Registration for IPv4 care-of address

If the home agent rejects the IPv4 care-of address, it MUST store the error code value in the Status field of the BID mobility option.

8.2. IPv4 HoA Management

When the mobile node wants to configure an IPv4 home address in addition to the IPv6 home address, it can request for one using the IPv4 Home Address option in the Binding Update. If the home agent accepts the Binding Update, the mobile node can now register multiple care-of addresses for the IPv4 home address in addition to the IPv6 home address. The same set of care-of addresses will be registered for both IPv6 and IPv4 home addresses. The mobile node cannot bind different set of care-of addresses to each home address.

According to [ID-DSMIPv6], the home agent includes the IPv4 address acknowledgement option in the Binding Acknowledgement only if the mobile node had requested for an IPv4 home address in the corresponding Binding Update. The IPv4 address acknowledgement option MUST be present before any BID option. The status field of the IPv4 address acknowledgement option contains only the error code corresponding to the IPv4 home address management. The error values related to the IPv4 care-of address registration MUST be stored in the BID mobility option.

9. IPsec and IKEv2 interaction

Mobile IPv6 [RFC-3775] and the NEMO protocol [RFC-3963] require the use of IPsec to protect signaling messages like Binding Updates, Binding Acknowledgements and return routability messages. IPsec may also be used protect all tunneled data traffic. The Mobile IPv6-IKEv2 specification [RFC-4877] specifies how IKEv2 can be used to setup the required IPsec security associations. The following assumptions were made in [RFC-3775], [RFC-3963] and [RFC-4877] with respect to the use of IKEv2 and IPsec.

- There is only one primary care-of address per mobile node.
- The primary care-of address is stored in the IPsec database for tunnel encapsulation and decapsulation.
- When the home agent receives a packet from the mobile node, the source address is verified against the care-of address in the corresponding binding cache entry. If the packet is a reverse tunneled packet from the mobile node, the care-of address check is done against the source address on the outer IPv6 header. The reverse tunnel packet could either be a tunneled HoTi message or tunneled data traffic to the correspondent node.
- The mobile node runs IKEv2 (or IKEv1) with the home agent using the care-of address. The IKE SA is based on the care-of address of the mobile node.

The above assumptions may not be valid when multiple care-of addresses are used by the mobile node. In the following sections, the main issues with the use of multiple care-of address with IPsec are addressed.

9.1. Use of Care-of Address in the IKEv2 exchange

For each home address the mobile node sets up security associations with the home agent, the mobile node must pick one care-of address and use that as the source address for all IKEv2 messages exchanged to create and maintain the IPsec security associations associated with the home address. The resultant IKEv2 security association is created based on this care-of address.

If the mobile node needs to change the care-of address, it just sends a Binding Update with the care-of address it wants to use, with the corresponding Binding Identifier mobility option, and with the 'K' bit set. This will force the home agent to update the IKEv2 security association to use the new care-of address. If the 'K' bit is not supported on the mobile node or the home agent, the mobile node MUST

re-establish the IKEv2 security association with the new care-of address. This will also result in new IPsec security associations being setup for the home address.

9.2. Transport Mode IPsec protected messages

For Mobile IPv6 signaling message protected using IPsec in transport mode, the use of a particular care-of address among multiple care-of addresses does not matter for IPsec processing.

For Mobile Prefix Discovery messages, [RFC-3775] requires the home agent to verify that the mobile node is using the care-of address that is in the binding cache entry that corresponds to the mobile node's home address. If a different address is used as the source address, the message is silently dropped by the home agent. This document requires the home agent implementation to process the message as long as the source address is one of the care-of addresses in the binding cache entry for the mobile node.

9.3. Tunnel Mode IPsec protected messages

The use of IPsec in tunnel mode with multiple care-of address introduces a few issues that require changes to how the mobile node and the home agent send and receive tunneled traffic. The route optimization mechanism described in [RFC-3775] mandates the use of IPsec protection in tunnel mode for the HoTi and HoT messages. The mobile node and the home agent may also choose to protect all reverse tunneled payload traffic with IPsec in tunnel mode. The following sections address multiple care-of address support for these two types of messages.

9.3.1. Tunneled HoTi and HoT messages

The mobile node MAY use the same care-of address for all HoTi messages sent reverse tunneled through the home agent. The mobile node may use the same care-of address irrespective of which correspondent node the HoTi message is being sent. RFC 3775 requires the home agent to verify that the mobile node is using the care-of address that is in the binding cache entry, when it receives a reverse tunneled HoTi message. If a different address is used as the source address, the message is silently dropped by the home agent. This document requires the home agent implementation to decapsulate and forward the HoTi message as long as the source address is one of the care-of addresses in the binding cache entry for the mobile node.

When the home agent tunnels a HoT message to the mobile node, the care-of address used in the outer IPv6 header is not relevant to the HoT message. So regular IPsec tunnel encapsulation with the care-of

address known to the IPsec implementation on the home agent is sufficient.

9.3.2. Tunneled Payload Traffic

When the mobile sends and receives multiple traffic flows protected by IPsec to different care-of addresses, the use of the correct care-of address for each flow becomes important. Support for this requires the following two considerations on the home agent.

- When the home agent receives a reverse tunneled payload message protected by IPsec in tunnel mode, it must check that the care-of address is one of the care-of addresses in the binding cache entry. According to RFC 4306, the IPsec implementation on the home agent does not check the source address on the outer IPv6 header. Therefore the care-of address used in the reverse tunneled traffic can be different from the care-of address used as the source address in the IKEv2 exchange. However, the Mobile IPv6 stack on the home agent MUST verify that the source address is one of the care-of addresses registered by the mobile node before decapsulating and forwarding the payload traffic towards the correspondent node.

- For tunneled IPsec traffic from the home agent to the mobile node, The IPsec implementation on the home agent may not be aware of which care-of address to use when performing IPsec tunnel encapsulation. The Mobile IP stack on the home agent must specify the tunnel end point for the IPsec tunnel. This may require tight integration between the IPsec and Mobile IP implementations on the home agent.

10. Security Considerations

The security considerations for securing the Binding Update and binding acknowledgement messages with multiple care-of address are very similar to the security considerations for securing the Binding Update and binding acknowledgement. Please see [RFC-3775] for more information. The Binding Update and binding acknowledgement messages with multiple care-of addresses MUST be protected using IPsec as show in Section 9. Additional security considerations are described below.

With simultaneous binding support, it is possible for a malicious mobile node to successfully bind a number of victims' addresses as valid care-of addresses for the mobile node with its home agent. Once these addresses have been bound, the malicious mobile node can perform a re-direction attack by instructing the home agent (e.g. setting filtering rules to direct a large file transfer) to tunnel packets to the victims' addresses. Such risk is highlighted in [ID-MIP6ANALYSIS]. These attacks are possible because the care-of addresses sent by the mobile node in the Binding Update messages are not verified by home agent, i.e., the home agent does not check if the mobile node is at the care-of address it is claiming to be. The security model for Mobile IPv6 assumes that there is a trust relationship between the mobile node and its home agent. Any malicious attack by the mobile node is traceable by the home agent. This acts as a deterrent for the mobile node to launch such attacks.

Although such risk exists in Mobile IPv6, the risk level is escalated when simultaneous multiple care-of address bindings are performed. In Mobile IPv6, a mobile node can only have a single care-of address binding per home address at a given time. However, for simultaneous multiple care-of address bindings, a mobile node can have more than one care-of address binding per home address at a given time. This implies that a mobile node using simultaneous binding support can effectively bind more than a single victim's address. Another difference is the degree of risk involved. In the single care-of address binding case, once the re-direction attack is initiated, a malicious mobile node would be unable to use its home address for communications (such as to receive control packets pertaining to the file transfer). However, in the simultaneous binding support case, a malicious mobile node could bind a valid care-of address in addition to multiple victims addresses. This valid care-of address could then be used by the malicious mobile node to set up flow filtering rules at its home agent, thereby controlling and/or launching new re-direction attacks.

Thus, in view of such risks, it is advisable for a home agent to employ some form of care-of address verification mechanism before

using the care-of addresses as a valid routing path to a mobile node. Solutions related to this are described in [ID-COAVERIFY].

11. IANA Considerations

The following Extension Types MUST be assigned by IANA:

- Binding Identifier mobility option type: This must be assigned from the same space as mobility option in [RFC-3775].

- New Successful Status of Binding Acknowledgement: This status code must be assigned from the same space as binding acknowledgement status codes in [RFC-3775].

  * MCOA NOTCOMPLETE (TBD)

  * MCOA RETURNHOME WO/NDP (TBD)

- New Unsuccessful Status of Binding Acknowledgement: These status codes must also be assigned from the same space as binding acknowledgement status codes in [RFC-3775].

  * MCOA MALFORMED (TBD)

  * MCOA BID CONFLICT (TBD)

  * MCOA PROHIBITED(TBD)

  * MCOA BULK REGISTRATION NOT SUPPORTED (TBD)

12. Acknowledgements

The authors would like to special thank George Tsirtsis for thorough review and suggestions. The authors would also like to thank Masafumi Aramoto, Keigo Aso, Julien Charbon, Tero Kauppinen, Benjamin Lim, Martti Kuparinen, Romain Kuntz, Heikki Mahkonen, Nicolas Montavont for their discussions and inputs. Thanks to Susumu Koshiba, Hiroki Matutani, Koshiro Mitsuya, Koji Okada, Keisuke Uehara, Masafumi Watari and Jun Murai for earlier work on this subject.

13. References

13.1. Normative References

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

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

[RFC-2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

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

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

[RFC-4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the revised IPsec Architecture", RFC 4877, April 2007.

13.2. Informative References

[ID-MOTIVATION] Ernst, T., Montavont, N., Wakikawa, R., Ng, C., and K. Kuladinithi, "Motivations and Scenarios for Using Multiple Interfaces and Global Addresses", draft-ietf-monami6-multihoming-motivation-scenario-02 (work in progress), July 2007

[RFC-4980] Ng, C., Paik, Ernst, and C. Bagnulo, "Analysis of Multihoming in Network Mobility Support", RFC 4980, October 2007.

[ID-MIP6ANALYSIS] Montavont, N., Wakikawa, R., Ernst, T., Ng, C., and

K. Kuladinithi, "Analysis of Multihoming in Mobile IPv6", draft-ietf-monami6-mipv6-analysis-04 (work in progress), Novemver 2007.

[RFC-3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC-4885] Ernst, T. and H. Lach, "Network Mobility Support Terminology", RFC 4885, July 2007.

[ID-DSMIPv6] Soliman, H., "Mobile IPv6 support for dual stack Hosts and Routers (DSMIPv6)", draft-ietf-mext-v4traversal-01 (work in progress), February 2008.

[ID-COAVERIFY] Lim, B., C. NG and K. Aso, "Verification of Care-of Addresses in Multiple Bindings Registration", draft-lim-mext-multiple-coa-verify-01 (work in progress), February 2008.

[RFC-4068bis] R. Koodli, "Mobile IPv6 Fast Handovers", draft-ietf-mipshop-fmipv6-rfc4068bis-07.txt (work in progress), April 2008.

Authors' Addresses

Ryuji Wakikawa
Toyota ITC / Keio University
6-6-20 Akasaka, Minato-ku
Tokyo 107-0052
Japan

Phone: +81-3-5561-8276
Fax: +81-3-5561-8292
Email: ryuji@jp.toyota-itc.com

Thierry Ernst
INRIA
INRIA Rocquencourt
Domaine de Voluceau B.P. 105
Le Chesnay, 78153
France

Phone: +33-1-39-63-59-30
Fax: +33-1-39-63-54-91
Email: thierry.ernst@inria.fr
URI: http://www.nautilus6.org/~thierry

Kenichi Nagami
INTEC NetCore Inc.
1-3-3, Shin-suna
Koto-ku, Tokyo 135-0075
Japan

Phone: +81-3-5565-5069
Fax: +81-3-5565-5094
Email: nagami@inetcore.com

Vijay Devarapalli
Wichorus
3590 North First St
San Jose, CA 95134
USA

Email: vijay@wichorus.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to 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).