

Network Working Group
Request for Comments: 5648
Category: Standards Track

R. Wakikawa, Ed.
Toyota ITC
V. Devarapalli
Wichorus
G. Tsirtsis
Qualcomm
T. Ernst
INRIA
K. Nagami
INTEC NetCore
October 2009

Multiple Care-of Addresses Registration

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, 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.

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright and License Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Protocol Overview	4
4. Mobile IPv6 Extensions	10
4.1. Binding Cache Structure and Binding Update List	10
4.2. Binding Update Message	10
4.3. Binding Identifier Mobility Option	11
4.4. New Status Values for Binding Acknowledgement	13
5. Mobile Node Operation	14
5.1. Management of Care-of Address(es) and Binding Identifier(s)	14
5.2. Binding Registration	15
5.3. Bulk Registration	16
5.4. Binding De-Registration	16
5.5. Returning Home with Complete Binding De-Registration: Using a Single Interface	17
5.5.1. Using Only the Interface Attached to the Home Link	17
5.5.2. Using Only the Interface Attached to the Visited Link	17
5.6. Returning Home: Simultaneous Home and Visited Link Operation	18
5.6.1. Problems of Simultaneous Home and Foreign Attachments	18
5.6.2. Overview and Approach	18
5.6.3. Home Binding Support	19
5.6.4. Sending Packets from the Home Link	20
5.6.5. Leaving from the Home Link	20
5.7. Receiving Binding Acknowledgement	21
5.8. Receiving Binding Refresh Request	22
5.9. Bootstrapping	22
6. Home Agent and Correspondent Node Operation	22
6.1. Searching Binding Cache with Binding Identifier	22
6.2. Processing Binding Update	23
6.3. Sending a Binding Acknowledgement for Home Link Registration	25
6.4. Sending Binding Refresh Request	27
6.5. Receiving Packets from Mobile Node	27
7. Network Mobility Applicability	27
8. DSMIPv6 Applicability	27
8.1. IPv4 Care-of Address Registration	28
8.2. IPv4 Home Address Management	29

9. IPsec and IKEv2 Interaction	30
9.1. Use of Care-of Address in the IKEv2 Exchange	31
9.2. Transport Mode IPsec-Protected Messages	31
9.3. Tunnel Mode IPsec-Protected Messages	31
9.3.1. Tunneled Home Test Init and Home Test Messages	31
9.3.2. Tunneled Payload Traffic	32
10. Security Considerations	33
11. IANA Considerations	34
12. Acknowledgements	35
13. References	35
13.1. Normative References	35
13.2. Informative References	35

1. Introduction

A mobile node may use various types of network interfaces to obtain durable and wide area network connectivity. This has 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 [MOTIVATION]. When a mobile node with multiple interfaces uses Mobile IPv6 [RFC3775] 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 bind only one care-of address at a time with its home address. See [MIP6ANALYSIS] for a further analysis of using multiple interfaces and addresses with Mobile IPv6.

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 is sent in the Binding Update. The home agent that receives this Binding Update creates a 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 [RFC2119].

Terms used in this document are defined in [RFC3775], [RFC3753], and [RFC4885]. In addition to or as a 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. BIDs assigned to the same home address must not be duplicated at the same time. The value zero is reserved for future extensions. 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 of 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 5.3. A mobile node must not perform the bulk registration mechanism described in this specification with a correspondent node.

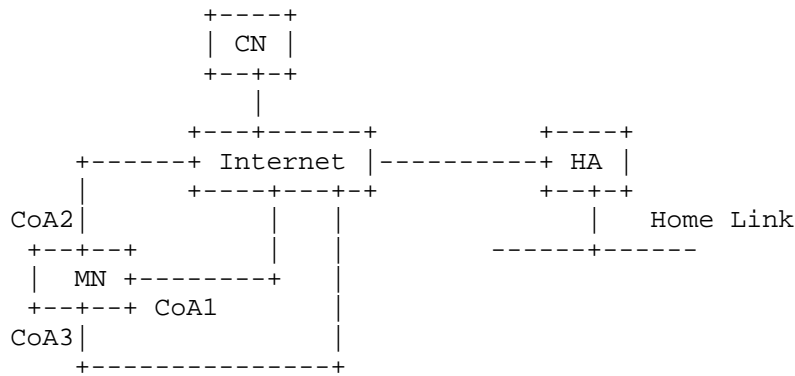
3. Protocol Overview

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 either register multiple care-of addresses at once in a single Binding Update or independently in individual Binding Updates.

If the mobile host wishes to register its binding with a correspondent node, it must perform return routability operations as described in [RFC3775]. This includes managing a Care-of Keygen token per care-of address and exchanging Care-of Test Init and Care-of Test messages 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 [RFC3775] 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 addresses. In Figure 1, the home address of the mobile node (MN) is 2001:db8::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 [2001:db8::EUI  BID1 care-of address1]
  binding [2001:db8::EUI  BID2 care-of address2]
  binding [2001:db8::EUI  BID3 care-of address3]
correspondent node's binding
  binding [2001:db8::EUI  BID1 care-of address1]
  binding [2001:db8::EUI  BID2 care-of address2]
  binding [2001:db8::EUI  BID3 care-of address3]
  
```

Figure 1: Multiple Care-of Addresses Registration

If the mobile node decides to act as a regular mobile node compliant with [RFC3775], it sends a Binding Update without any Binding Identifier mobility options. The receiver of the Binding Update deletes all the bindings registered 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.

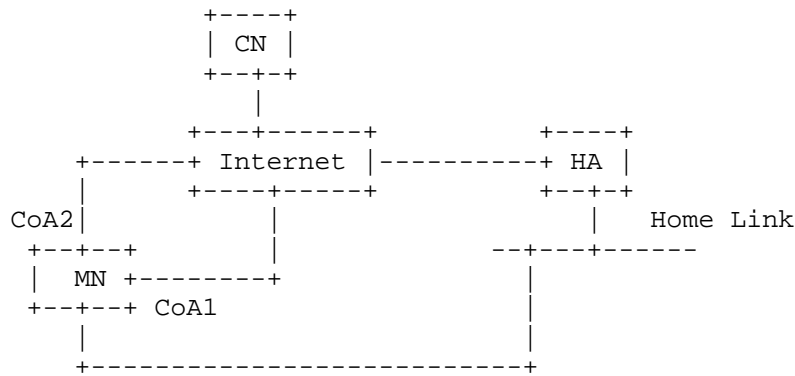
Binding cache lookup is done based on the home address and BID information if a BID is available. This is different from RFC 3775, where only the home address is used for binding cache lookup. Binding cache lookup is operated for either protocol signaling or data packets. For protocol signaling such as a Binding Update, BID should be always carried by a BID sub-option in a protocol signaling. Therefore, a correspondent binding cache that matches the specified BID MUST be found from the binding cache database. On the other hand, for the data packets, no BID information is carried in a packet. The binding cache lookup may involve policy or flow filters to retrieve a correspondent BID per packet in cases where some policy or flow filters are used to direct a certain packet or flow to a particular care-of address. However, the binding cache lookup using policy or flow filters is out of scope for this document. If no such

mechanism is available and no BID is found for a packet, a node SHOULD use the binding that was last verified by receiving data packets or signaling from the mobile node. In case the binding cache lookup for data packets, using the combination of home address and BID, does not return a valid binding cache entry, the home agent SHOULD perform the lookup based on only the home address as described in [RFC3775].

In any case, to avoid problems with upper-layer protocols and TCP in particular, a single packet flow as identified by the 5-tuple SHOULD only be sent to a single care-of address at a time.

The mobile node may return to the home link through one of its interfaces. There are two options possible for the mobile node when it returns home. Sections 5.5.1 and 5.6 describe the returning-home procedures in more detail.

1. The mobile node uses only the interface with which it attaches to the home link and takes back full ownership of its HoA (home address) on 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 nodes 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 from and to each care-of address directly.



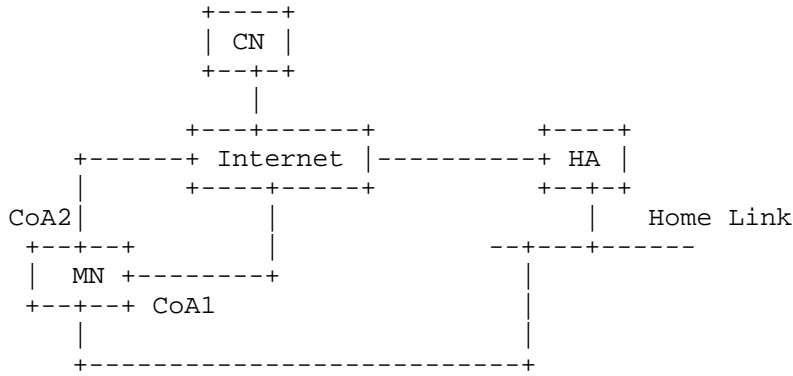
```

Binding Cache Database:
home agent's binding
  none
correspondent node's binding
  binding [2001:db8::EUI BID1 care-of address1]
  binding [2001:db8::EUI BID2 care-of address2]
  
```

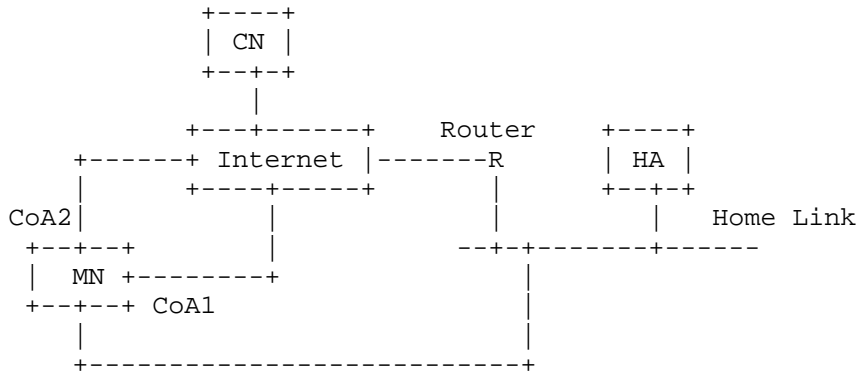
Figure 2: Using Only an Interface Attached to the Home Link

2. 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 3. There are two possible topologies, depending on whether or not the home agent is the only router on the home link. The operation of Neighbor Discovery [RFC4861] is different in the two topologies. More details can be found in Section 5.6. The home agent and the correspondent node have the binding entries listed in Figure 3 in their binding cache database in both topologies. The home agent also knows that the mobile node is 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 to 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 for this document.

Topology-a)



Topology-b)



Binding Cache Database:

```

home agent's binding
  binding [2001:db8::EUI BID1 care-of address1]
  binding [2001:db8::EUI BID2 care-of address2]
correspondent node's binding
  binding [2001:db8::EUI BID1 care-of address1]
  binding [2001:db8::EUI BID2 care-of address2]
  
```

Figure 3: Simultaneous Home and Visited Link Operation

This specification keeps backwards compatibility with [RFC3775]. If a receiver (either home agent or correspondent node) does not support this specification, it does not understand the Binding Identifier mobility option. The receiver skips the unknown mobility option (i.e., the Binding Identifier mobility option) and processes the Binding Update as defined in [RFC3775]. In order to keep backwards compatibility with [RFC3775], when a mobile node sends a Binding

Update message with extensions described in this document, the receiver needs to reflect the Binding Identifier mobility option in the Binding Acknowledgement. If the mobile node finds no Binding Identifier mobility options in the received Binding Acknowledgement, it assumes the other end node does not support this specification. In such case, the mobile node needs to fall back to the legacy [RFC3775]-compliant mobile node. If it is the home registration, the mobile node MAY try to discover another home agent that supports the Binding Identifier mobility option for the home registration.

4. Mobile IPv6 Extensions

This section summarizes the extensions to Mobile IPv6 that are necessary to 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 MUST 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 an individual or a bulk Binding Update, the sequence number is incremented. When a home agent receives an individual Binding Update, it should update the sequence number for all the bindings for a particular mobile node, with the sequence number in the received Binding Update.

4.2. Binding Update Message

This specification extends the Binding Update message with a new flag. The flag is shown and described below.

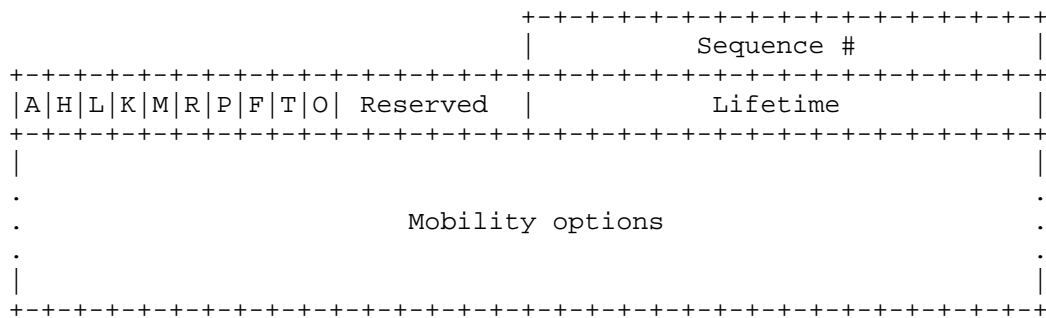


Figure 4: Binding Update Message

Overwrite (O) flag

When this flag is set, all the binding cache entries for a mobile node are replaced by new entries registering with this Binding Update message. This flag is only used when the BID mobility option is carried with the Binding Update.

Reserved

6-bit Reserved field.

4.3. 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 messages. The Binding Identifier mobility option has an alignment requirement of 2n if the Care-of Address field is not present. Otherwise, it has the alignment requirement of 8n + 2.

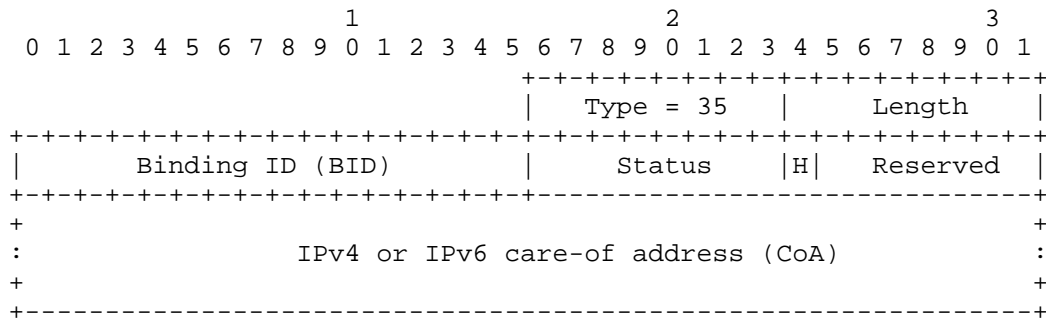


Figure 5: BID Mobility Option

Type

Type value for Binding Identifier is 35.

Length

8-bit unsigned integer. Length of the option, in octets, excluding the Type and Length fields. It MUST be set to either 4, 8, 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 8. Otherwise, the length value MUST be set to 20 for IPv6 care-of addresses.

Binding ID (BID)

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

Status

The Status field is an 8-bit unsigned integer. When the Binding Identifier mobility option is included in a Binding Acknowledgement, this field overwrites the Status field in the Binding Acknowledgement only for this BID. If this field is set to zero, the receiver ignores this field and uses the registration status stored in the Binding Acknowledgement message. The receiver MUST ignore this field if the Binding Identifier mobility option is not carried within either the Binding Acknowledgement or the Care-of Test messages. The possible status codes are the same as the status codes of the Binding Acknowledgement. This Status field is also used to carry error information related to the care-of address test in the Care-of Test message.

Simultaneous Home and Foreign Binding (H) flag

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

Reserved

7-bit Reserved field. The value MUST be initialized to zero by the sender, and SHOULD be ignored by the receiver.

Care-of Address

If a Binding Identifier mobility option is included in a Binding Update for the home registration, either IPv4 or IPv6 care-of addresses for the corresponding BID can be stored in this field. For the binding registration to correspondent nodes (i.e., route optimization), only IPv6 care-of addresses can be stored in this field. If no address is specified in this field, the length of this field MUST be zero (i.e., not appear in the option). If the option is included in any messages other than a Binding Update, the length of this field MUST also be zero.

4.4. 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 (4)

In bulk registration, not all the Binding Identifier mobility options were successfully registered. Some of them were 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 (5)

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

MCOA MALFORMED (164)

Registration failed because the Binding Identifier mobility option was not formatted correctly. This value is used in the following cases:

- * when the wrong length value is specified (neither 4, 8, nor 20) in the Length field of the Binding Identifier mobility option.
- * when a unicast routable address is not specified in the Care-of Address field of the Binding Identifier mobility option.
- * when a care-of address does not appear in the Care-of Address field of the Binding Identifier mobility option stored in an IPsec Encapsulating Security Payload (ESP)-protected Binding Update.

MCOA NON-MCOA BINDING EXISTS (165)

Indicates that a bootstrapping multiple care-of addresses registration was performed without the 'O' flag set.

MCOA UNKOWN COA (167)

Indicates that a Binding Identifier mobility option did not include a Care-of Address field and that the receiver has no record for the Binding ID indicated in the same option.

MCOA PROHIBITED (166)

Implies that the multiple care-of addresses registration is administratively prohibited.

MCOA BULK REGISTRATION PROHIBITED (168)

Bulk binding registration is either not permitted or not supported. Note that the bulk registration is an optional procedure and might not be available on a home agent.

MCOA SIMULTANEOUS HOME AND FOREIGN PROHIBITED (169)

Simultaneous home and foreign attachment is neither supported nor permitted.

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. A mixture of the two cases is also possible. Note that a mobile node can use BID regardless of the number of interfaces and care-of addresses. Whether or not a mobile node uses BID is determined by a local configuration.

1. A mobile node is 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 to which the interface is attached. 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 is 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. The value is an integer between 1 and 65535. A zero value SHOULD NOT be used as a BID. 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 with which to register, at which time all of the care-of addresses MUST be mapped to BIDs.

When a mobile node registers a given BID for the first time, it MUST include the Care-of Address field in the Binding Identifier mobility option. For any subsequent registrations that either re-register or de-register the same BID, the MN need not include the Care-of Address field in the Binding Identifier mobility option.

5.2. 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.

When IPsec ESP is used for protecting the Binding Update, a care-of address MUST be carried in an alternate Care-of Address mobility option as described in [RFC4877]. However, in this specification, the care-of address MUST be carried in the Care-of Address field of the Binding Identifier mobility option. In order to save bits of the Binding Update, the alternate Care-of Address option MUST NOT be included.

For binding registration to a correspondent node, the mobile node MUST have both active Home and Care-of Keygen tokens for Kbm (binding management key; see Section 5.2.5 of [RFC3775]) 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.

```

    IPv6 header (src=Care-of Address, dst=Home Agent Address)
    IPv6 Home Address Option
    ESP Header*
    Mobility header
      Binding Update
      Mobility Options
        Binding Identifier mobility option
        Binding Authorization mobility option+
  (*) if necessary, for home registration
  (+) if necessary, for route optimization

```

Figure 6: Binding Update for Binding Registration

If the mobile node wants to replace existing registered bindings on the home agent with the single binding in the sent Binding Update, it sets the 'O' flag. If the 'O' flag is not set, then the binding will be added to existing bindings in the home agent. The single binding will be registered with the assigned BID. Section 6.2 describes this registration procedure in detail.

5.3. 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 it wants to register in the same Binding Update message. As with single registrations (see Section 5.1), the Care-of Address field is included for each BID registered for the first time. 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.

```

IPv6 header (src=Care-of Address, dst=Home Agent Address)
  IPv6 Home Address Option
  ESP Header
  Mobility header
    Binding Update
    Mobility Options
      Binding Identifier1 (including Care-of Address)
      Binding Identifier2 (including Care-of Address)
      Binding Identifier3 (no Care-of Address)
      Binding IdentifierN (no Care-of Address)
  :

```

Figure 7: Binding Update for Bulk Registration

As with regular registrations, if the mobile node wants to replace existing registered bindings on the home agent with the multiple bindings in the sent Binding Update, it sets the 'O' flag in the Binding Update; otherwise, the bindings are added to the existing bindings in the home agent.

5.4. 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 [RFC3775]. 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). Since de-registration attempts to remove a BID that already exists, the Care-of Address field in each Binding Identifier option can be omitted by the sender as defined in Section 5.1.

5.5. Returning Home with Complete Binding De-Registration: Using a Single Interface

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.

5.5.1. Using Only the Interface Attached to the Home Link

The mobile node returns home and de-registers all the bindings it has with the home agent, as shown in Figure 2 and as defined in [RFC3775]. 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, to the correspondent node, bindings for interfaces attached to visited links as shown in Figure 2.

5.5.2. Using Only the Interface Attached to the Visited Link

The mobile node returns home physically but shuts down the interface attached to the home link. As a result, a mobile node does not return home even though it attaches to the home link by one of the interfaces. Before shutting down the interface, any binding for the care-of address previously associated with the interface should be deleted as defined in Section 5.4.

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. Returning Home: Simultaneous Home and Visited Link Operation

5.6.1. 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 3.

In [RFC3775], the home agent intercepts packets meant for the mobile node using proxy Neighbor Discovery [RFC4861] 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 and 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 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. Deployments making use of multiple care-of addresses are required to avoid configuration 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.

5.6.2. Overview and Approach

The home agent MUST intercept all the packets meant for the mobile node, whether or not the mobile node is attached to the home link, and decide whether to send the traffic directly to the home address on the link or tunnel to the care-of address.

Two scenarios are illustrated in Figure 3, depending on whether or not the home agent is the only router at the home link. 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 3). 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. However, there is one limitation of this scenario. If a correspondent node is located at the home link, the home agent may not intercept the packets destined to

the mobile node. These packets are routed only via the home link, but this is the most optimal path for the mobile node to communicate with nodes on the home link.

2. If there are routers other than the home agent on the home link, 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 the 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 the Mobility Header Link-Layer Address option defined in [RFC5568] 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 [RFC3775] when a mobile node sends a de-registration Binding Update to the home agent's link-layer address in the operation for returning home.

5.6.3. Home Binding Support

When the home binding is used, the mobile node MUST send a registering Binding Update with a Binding Identifier mobility option with the 'H' flag set. The lifetime MUST be set to a non-zero lifetime of the home binding, and the Care-of Address field MUST be set to the home address. The mobile node registers only one home binding at a time, even if it attaches to the home link by multiple interfaces.

The mobile node SHOULD include the Mobility Header Link-Layer Address option [RFC5568] to notify the mobile node's link-layer address to the home agent, too. The option code of the Mobility Header Link-Layer Address 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 [RFC3775], the mobile node MUST start responding to Neighbor Solicitation for its home address right after it sends the de-registration 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 (5)] status value in the received Binding Acknowledgment, it MUST NOT respond to Neighbor Solicitation even after the Binding Acknowledgement.

The management of the home binding is the same as the binding management described in this specification. The home binding can be included in a bulk binding registration (Section 5.3). The MN SHOULD refresh the lifetime of the home binding by sending appropriate Binding Updates as with any other binding.

5.6.4. Sending Packets from the Home Link

- o 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 were a regular IPv6 node.
- o 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 to include a 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 receives the de-registration Binding Update message. Note that the default router MUST NOT cache the mobile node's link-layer address in the neighbor cache when it forwards the packet from the mobile node to the home agent.

5.6.5. Leaving from the Home Link

When the mobile node detaches from the home link, it SHOULD immediately send a Binding Update for one of the active care-of addresses with the 'H' flag unset. When the 'H' flag of the BID option is unset in any Binding Update, the home agent stops forwarding the mobile node's packets to 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 [RFC3775]). The operation for sending a Binding Acknowledgement is described in Section 6.2.

If a mobile node includes a Binding Identifier mobility option in a Binding Update with the 'A' flag set, a Binding Acknowledgement SHOULD carry a Binding Identifier mobility option. According to [RFC3775], the receiver of the Binding Update ignores unknown mobility options and processes the Binding Update without the unknown mobility option. Therefore, if no such mobility option is included in the Binding Acknowledgement in response to a Binding Update for a multiple care-of addresses registration, this indicates that the originating node of the Binding Acknowledgement does not support processing the Binding Identifier mobility option regardless of status value. In such case, the receiver of the Binding Update may create a regular binding. The mobile node then SHOULD no longer attempt a multiple care-of addresses registration with that node. If this occurs with home registration, the mobile node MAY attempt to discover another home agent that supports the Binding Identifier mobility option for the home registration.

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.

- o If the status value is [MCOA PROHIBITED], the mobile node MUST stop registering multiple bindings with the node that sent the Binding Acknowledgement.
- o If the status value is [MCOA BULK REGISTRATION PROHIBITED], the mobile node needs to stop using bulk registrations with the node that sent the Binding Acknowledgement. It should assume that none of the attempted registrations were successful.
- o If [MCOA MALFORMED] is specified, it indicates that the Binding Identifier mobility option is formatted wrong, presumably due to a programming error or major packet corruption.

- o If [MCOA NON-MCOA BINDING EXISTS] is specified, it means that there is a non-MCoA binding entry in the receiver. The mobile node MUST set 'O' flag so that all the registered bindings are replaced by an MCoA registration as described in Section 5.9.
- o If [MCOA UNKNOWN COA] is specified, it means that the mobile node sent a Binding Identifier mobility option without a Care-of Address field, but the receiver could not find an entry for the BID indicated. If the mobile node is trying to de-register a BID, it need not do anything further. If the mobile node is trying to refresh a binding, it SHOULD send a Binding Identifier mobility option including the Care-of Address field.

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 [RFC3775]). The operation of sending a Binding Refresh Request is described in 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 that the mobile node send a new Binding Update for the BID. The mobile node SHOULD then send a Binding Update at least for the respective binding, as described in Sections 5.2 and 5.3.

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 Update message. If old bindings still exist 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 loses state regarding the registrations. If the 'O' flag is set, all the bindings are replaced by the new binding(s).

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

```
binding1 [2001:db8::EUI, care-of address1, BID1]
binding2 [2001:db8::EUI, care-of address2, BID2]
binding3 [2001:db8::EUI, care-of address3, BID3]
```

Figure 8: Searching the Binding Cache

The node learns the BID when it receives a Binding Identifier mobility option. At that time, the node MUST look up its binding cache database with the home address and the BID retrieved from the Binding Update. If the 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 node does not desire to use multiple bindings for a mobile node, it can simply ignore the BID.

6.2. Processing Binding Update

If a Binding Update does not contain a Binding Identifier mobility option, its processing is the same as in [RFC3775]. If the receiver already has multiple bindings for the home address, it MUST replace all the existing bindings with the received binding. If the [RFC3775] Binding Update is for de-registration, the receiver MUST delete all existing bindings from its binding cache.

If the Binding Update contains Binding Identifier mobility option(s), it is first validated according to Section 9.5.1 of [RFC3775]. Then the receiver processes the Binding Identifier mobility option(s) as described in the following steps.

- o 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 return the status value set to [MCOA MALFORMED].
- o When the length value is either 8 or 20, the care-of address MUST be present in the Binding Identifier mobility option. If the unicast routable address [RFC3775] is not present in the Care-of Address field, the receiver MUST reject the Binding Identifier mobility option and return the status value set to [MCOA MALFORMED].

- o 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 return the status value set to [MCOA BULK REGISTRATION PROHIBITED] in the binding Acknowledgement.
- o 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].
- o 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 MUST follow the descriptions described in Section 5.6.
- o 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 the IPv6 address copied from the Care-of Address field in the Binding Identifier mobility option.
 - * When the length value is 8, the address MUST be the IPv4 valid address. How to obtain an IPv4 care-of address is described in Section 8.
 - * When the length value is 4 and the Binding Identifier is present in the binding cache, the receiving node MUST update the associated binding entry. Otherwise, the receiving node MUST reject that Binding Identifier mobility option and send a Binding Acknowledgement with the status for that Binding Identifier mobility option set to [MCOA UNKNOWN].
- o Once the care-of address(es) have been retrieved from the Binding Update, the receiving nodes create new binding(s).
 - * If the 'O' flag is set in the Binding Update, the receiving node removes all the existing bindings and registers the received binding(s).

- * If the 'O' flag is unset in the Binding Update and the receiver has a regular binding that does not have a BID for the mobile node, it must not process the Binding Update. The receiver should send a Binding Acknowledgement with status set to [MCOA NON-MCOA BINDING EXISTS].
- * 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 and the 'A' flag is set in the Binding Update, 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, MAY 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 always be stored in the Status field of the Binding Acknowledgement and the Status field of the Binding Identifier mobility option MUST always be set to zero.

When the home agent sends a Binding Acknowledgement, 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 the 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, the Status field of the Binding Acknowledgement MUST be set to [MCOA NOTCOMPLETE], so that the receiver can examine the Status field of each Binding Identifier mobility option for further operations. Otherwise, the Status field of the Binding Identifier mobility option MUST be set to zero and the home agent Status field of the Binding Acknowledgement is used.

6.3. Sending a Binding Acknowledgement for Home Link Registration

The operations described in this section are related to returning home with simultaneous use of home and foreign links.

- o When the home agent sends the Binding Acknowledgement after successfully processing the home binding registration, it MUST set the status value to either 0 [Binding Update Accepted] or [MCOA RETURNHOME WO/NDP (5)] 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): The Neighbor Discovery protocol is permitted for the home address at the home link. This is the regular returning home operation of [RFC3775].
 - * MCOA RETURNHOME WO/NDP (5): The Neighbor Discovery protocol is prohibited for the home address at the home link.

The respective Binding Identifier mobility options need to be included in the Binding Acknowledgement.

- o If the Binding Update is rejected, the appropriate error value MUST be set in the Status field. In this case, the home agent operation is the same as in [RFC3775].
- o Only if the home agent is the only router in the home link MAY it turn off Neighbor Discovery for the requested home address and respond 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 Mobility Header Link-Layer Address option [RFC5568] in the received Binding Update. After the completion of the home binding registration, 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.
- o If the home agent is not the only router in the home link, the home agent returns [MCOA RETURNHOME WO/NDP] value in the Status field of the Binding Identifier mobility option. The home agent learns the mobile node's link-layer address by receiving the Mobility Header 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.
- o Note that the use of proxy Neighbor Discovery is an 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].

- o If the BID option is not included in the Binding Acknowledgement, the home agent might not recognize the home registration. The home agent might have processed the home registration Binding Update as a regular de-registration, as described in [RFC3775], and deleted all the registered binding cache entries for the mobile node. Thus, the mobile node SHOULD stop using the interface attached to the foreign link and use only the interface attached to the home link.

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. The node MAY include multiple Binding Identifier mobility options if there are multiple 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 is equal to one of the care-of addresses in the binding cache entry. If no binding is found, the packets MUST be discarded. The node MUST also send a Binding Error message as specified in [RFC3775]. 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 [RFC3963]. Therefore, the extensions described in this document can also be used to support a mobile router with multiple care-of addresses. [RFC4980] contains an analysis of NEMO multihoming.

8. DSMIPv6 Applicability

Dual Stack Mobile IPv6 (DSMIPv6) [RFC5555] 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 the multiple care-of addresses 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 addresses.

Bulk registration MUST NOT be used for the initial binding registration 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 [RFC5555] except that the IPv4 care-of address option MUST NOT be used when the BID mobility option is used.

```

    IPv4 header (src=V4ADDR, dst=HA_V4ADDR)
      UDP Header
        IPv6 header (src=V6HoA, dst=HAADDR)
          ESP Header
            Mobility header
              -Binding Update
            Mobility Options
              - Binding Identifier (IPv4 CoA)
    *V4ADDR, HA_V4ADDR, V6HOA, HAADDR are defined in [RFC5555]
```

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 an IPv4 care-of address, it MUST follow the format described in Figure 9. Note that the IPv4 care-of address must be registered by a non-bulk binding registration whenever it is changed.

As shown in Figure 9, the IPv4 care-of address will appear in the Binding Identifier mobility option. The IPv4 Care-of Address mobility option defined in [RFC5555] MUST always be omitted. The receiver of the Binding Update message for an IPv4 care-of address

MUST treat the IPv4 address stored in the Binding Identifier mobility option as the one in the IPv4 Care-of Address mobility option of [RFC5555]. If the IPv4 address in the Binding Identifier mobility option is different from one in the Source Address field in the IPv4 header of the Binding Update (i.e., V4ADDR in Figure 9), the source address is used as an IPv4 care-of address. Otherwise, the IPv4 address in the Binding Identifier mobility option is used as an IPv4 care-of address.

```

IPv6 header (src=Care-of Address, dst=Home Agent Address)
  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 an IPv4 Care-of Address

When the home agent returns a Binding Acknowledgement for the IPv4 care-of address registration, it SHOULD NOT use the IPv4 Address Acknowledgement mobility option and SHOULD use only the Binding Identifier mobility option. The registration status for the IPv4 care-of address is stored in the Status field of the Binding Identifier mobility option. However, if the home agent needs to store the status value specially defined for the IPv4 Address Acknowledgement mobility option, it MUST store the status value in the IPv4 Address Acknowledgement mobility option and MUST NOT store it in the Binding Identifier mobility option. In such case, the home agent MUST include both the IPv4 Address Acknowledgement mobility option and the Binding Identifier mobility option.

8.2. IPv4 Home Address Management

When the mobile node wants to configure an IPv4 home address in addition to the IPv6 home address, it can request 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 mobile node MUST always use the IPv4 Home Address mobility option for any purposes of the IPv4 home address management. The same set of care-of addresses will be registered for both IPv6 and IPv4 home addresses. The mobile node cannot bind a different set of care-of addresses to each home address.

According to [RFC5555], the home agent includes the IPv4 Address Acknowledgement option in the Binding Acknowledgement only if the mobile node had requested an IPv4 home address in the corresponding Binding Update. The IPv4 Address Acknowledgement option MUST be present before any Binding Identifier mobility option. The Status field of the IPv4 Address Acknowledgement option contains only the error code defined in Section 3.2.1 of [RFC5555]. The home agent MUST always include the IPv4 Address Acknowledgement mobility option in the Binding Acknowledgement for the IPv4 home address registration.

9. IPsec and IKEv2 Interaction

Mobile IPv6 [RFC3775] and the NEMO protocol [RFC3963] require the use of IPsec to protect signaling messages, including Binding Updates, Binding Acknowledgements, and return routability messages. IPsec may also be used to protect all tunneled data traffic. The Mobile IPv6-IKEv2 specification [RFC4877] specifies how IKEv2 can be used to set up the required IPsec security associations. The following assumptions were made in [RFC3775], [RFC3963], and [RFC4877] with respect to the use of IKEv2 and IPsec.

- o There is only one primary care-of address per mobile node.
- o The primary care-of address is stored in the IPsec database for tunnel encapsulation and decapsulation.
- o 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-tunneled packet could either be a tunneled Home Test Init message or tunneled data traffic to the correspondent node.
- o 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 addresses with IPsec are addressed.

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

For each home address for which 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 set up 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.

The home agent processes Mobile Prefix Discovery messages with the same rules of data packets described in Section 6.5.

9.3. Tunnel Mode IPsec-Protected Messages

The use of IPsec in tunnel mode with multiple care-of addresses 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 [RFC3775] mandates the use of IPsec protection in tunnel mode for the Home Test Init and Home Test 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 Home Test Init and Home Test Messages

The mobile node **MAY** use the same care-of address for all Home Test Init messages sent reverse tunneled through the home agent. The mobile node may use the same care-of address irrespective of which correspondent node the Home Test Init message is being to. 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 Home Test Init 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 Home Test Init 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 Home Test message to the mobile node, the care-of address used in the outer IPv6 header is not relevant to the Home Test 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 node 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.

- o When the home agent receives a reverse-tunneled payload message protected by IPsec in tunnel mode, the source address used in the outer IPv6 header is irrelevant to IPsec, since the tunnel mode security association is based on the addresses in the inner IPv6 header. Therefore, the same IPsec security association can be used for payload traffic tunneled from any of the care-of addresses. Note that 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, this does not cause an issue due to the above-mentioned reason.
- o For tunneled IPsec traffic from the home agent to the mobile node, the IPsec implementation on the home agent will not be aware of which care-of address to use when performing IPsec tunnel encapsulation. The Mobile IP stack on the home agent, based on the binding cache entries created by the mobile node, knows to which care-of address the packet belonging to a particular flow needs to be tunneled. The destination address for the outer IP header must either be conveyed dynamically per packet to the IPsec stack when it performs the encapsulation or the Mobile IPv6 stack must get access to the packet after IPsec processing is done and modify the destination address. The first option requires changes to the IPsec implementation. In the second option, there is a need for special processing in the forwarding function to replace the destination address on the outer header with the correct care-of address. The exact technique to achieve the above is implementation specific.

10. Security Considerations

The security considerations for securing the Binding Update and Binding Acknowledgement messages with multiple care-of addresses are very similar to the security considerations for securing the Binding Update and Binding Acknowledgement. Please see [RFC3775] for more information. The Binding Update and Binding Acknowledgement messages with multiple care-of addresses are securely exchanged as described in [RFC3775], [RFC4877], and Section 9 of this document. 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 [MIP6ANALYSIS]. These attacks are possible because the care-of addresses sent by the mobile node in the Binding Update messages are not verified by the home agent, i.e., the home agent does not check if the mobile node is at the care-of address at which it claims 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 a risk exists in Mobile IPv6, the risk level is increased 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. These mechanisms are out of scope for this document.

In the binding registration of Mobile IPv6, a care-of address is always verified by its reachability by a home agent. This reachability test may decrease the above risks. However, when bulk registration is used, a home agent cannot verify reachability of care-of addresses carried in a Binding Identifier mobility option. Therefore, the home agent can choose to reject bulk registration by using [MCOA BULK REGISTRATION PROHIBITED] in a Binding Acknowledgement. Alternatively, when a mobile node first registers a care-of address, it uses the individual Binding Updates for the first appeared care-of address. During the initial binding registration, a home agent can verify the address reachability for that given care-of address. After that, the mobile node uses bulk registration to refresh the care-of address.

11. IANA Considerations

The following Extension Types have been assigned by IANA:

- o Binding Identifier mobility option type: (35) has been assigned from the same space as the mobility option in [RFC3775].
- o New Successful Status of Binding Acknowledgement: These status codes have been assigned from the same space as the Binding Acknowledgement status codes in [RFC3775].
 - * MCOA NOTCOMPLETE (4)
 - * MCOA RETURNHOME WO/NDP (5)
- o New Unsuccessful Status of Binding Acknowledgement: These status codes have also been assigned from the same space as the Binding Acknowledgement status codes in [RFC3775].
 - * MCOA MALFORMED (164)
 - * MCOA NON-MCOA BINDING EXISTS (165)
 - * MCOA PROHIBITED (166)
 - * MCOA UNKNOWN COA (167)
 - * MCOA BULK REGISTRATION PROHIBITED (168)

* MCOA SIMULTANEOUS HOME AND FOREIGN PROHIBITED (169)

12. Acknowledgements

Ryuji Wakikawa and Thierry Ernst are grateful to Keio University for its initial support on this specification at the time when they were working there. In addition, the authors would like to thank Masafumi Aramoto, Keigo Aso, Julien Charbon, Tero Kauppinen, Martti Kuparinen, Romain Kuntz, Benjamin Lim, Heikki Mahkonen, Nicolas Montavont, and Chan-Wah Ng 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

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
- [RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
- [RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [RFC5555] Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.
- [RFC5568] Koodli, R., Ed., "Mobile IPv6 Fast Handovers", RFC 5568, July 2009.

13.2. Informative References

- [MOTIVATION] Ernst, T., Montavont, N., Wakikawa, R., Ng, C., and K. Kuladinithi, "Motivations and Scenarios for Using Multiple Interfaces and Global Addresses", Work in Progress, May 2008.

- [RFC4980] Ng, C., Ernst, T., Paik, E., and M. Bagnulo, "Analysis of Multihoming in Network Mobility Support", RFC 4980, October 2007.
- [MIP6ANALYSIS] Montavont, N., Wakikawa, R., Ernst, T., Ng, C., and K. Kuladinithi, "Analysis of Multihoming in Mobile IPv6", Work in Progress, May 2008.
- [RFC3753] Manner, J., Ed., and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, June 2004.
- [RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, July 2007.

Authors' Addresses

Ryuji Wakikawa (Editor)
TOYOTA InfoTechnology Center Co., Ltd.

E-Mail: ryuji.wakikawa@gmail.com (ryuji@jp.toyota-itc.com)

Vijay Devarapalli
Wichorus

E-Mail: vijay@wichorus.com

George Tsirtsis
Qualcomm

E-Mail: Tsirtsis@gmail.com

Thierry Ernst
INRIA

E-Mail: thierry.ernst@inria.fr

Kenichi Nagami
INTEC NetCore Inc.

E-Mail: nagami@inetcore.com

