MEXT WG
Internet-Draft
Intended status: Standards Track
Expires: February 1, 2009

A. Muhanna
M. Khalil
Nortel
S. Gundavelli
Cisco Systems
K. Chowdhury
Starent Networks
P. Yegani
Cisco Systems
July 31, 2008

Binding Revocation for IPv6 Mobility
draft-ietf-mext-binding-revocation-00.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 February 1, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document defines the revocation semantics for terminating a mobile node's mobility session and associated resources. These

semantics are generic enough and can be used by mobility entities in the case of Client Mobile IPv6 and its extensions. This mechanism allows the mobility entity which initiates the revocation procedure to request its corresponding one to terminate either one, multiple or all specified binding cache entries.

Table of Contents

1. Introduction 4
2. Conventions & Terminology 4
  2.1. Conventions used in this document 4
  2.2. Terminology 4
3. Binding Revocation Protocol and Use Cases Overview 4
  3.1. Binding Revocation Protocol 5
  3.2. Client MIPv6 and DSMIP6 Use Case 6
  3.3. Multi-Care of Addresses (Monami6) Use Case 7
    3.3.1. Termination of Multiple Care-of Addresses Bindings . . 7
    3.3.2. Termination of All Care-of Addresses Bindings 8
  3.4. Proxy MIPv6 Use Case 8
    3.4.1. Local Mobility Anchor Revokes A PMIPv6 Binding 8
    3.4.2. Local Mobility Anchor Revokes Bulk PMIPv6 Bindings . . 10
    3.4.3. Mobile Access Gateway Revoke Bulk PMIPv6 Bindings . . 10
4. Security Model 10
5. Binding Revocation Messages 10
  5.1. Binding Revocation Indication Message 10
  5.2. Binding Revocation Acknowledgement Message 13
6. Binding Revocation Process Considerations 15
  6.1. Sending Binding Revocation Messages 15
  6.2. Receiving Binding Revocation Messages 15
  6.3. Retransmission of Binding Revocation Indication 16
7. Home Agent Operation 16
  7.1. Sending Binding Revocation Indication 16
  7.2. Receiving Binding Revocation Acknowledgement 18
8. Local Mobility Anchor Operation 18
  8.1. Binding Revocation Initiator 18
    8.1.1. Sending Binding Revocation Indication 18
    8.1.2. Receiving Binding Revocation Acknowledgement 20
  8.2. Binding Revocation Responder 21
    8.2.1. Receiving Binding Revocation Indication 21
    8.2.2. Sending Binding Revocation Acknowledgement 22
9. Mobile Access Gateway Operation 23
  9.1. Binding Revocation Responder 23
    9.1.1. Receiving Binding Revocation Indication 23
    9.1.2. Sending Binding Revocation Acknowledgement 24
  9.2. Binding Revocation Initiator 25
    9.2.1. Sending Binding Revocation Indication 25
    9.2.2. Receiving Binding Revocation Acknowledgement 26

10. Mobile Node Operation 26
10.1. Receiving Binding Revocation Indication 26
10.2. Sending Binding Revocation Acknowledgement 27
11. Protocol Configuration Variables 28
12. IANA Considerations 28
13. Security Considerations 28
14. Acknowledgements 29
15. References 29
15.1. Normative References 29
15.2. Informative References 30
Authors' Addresses 30
Intellectual Property and Copyright Statements 32

1. Introduction

In the case of Mobile IPv6 and for administrative reason, sometimes it becomes necessary to inform the mobile node that its registration has been revoked and the mobile node is no longer able to receive IP mobility service using its Home Address. In some networks where Mobile IPv4 [RFC3344] has been deployed, a similar Mobile IPv4 registration revocation mechanism has been specified [RFC3543].

This document defines the semantics of the revocation mechanism of a mobile node registration binding, which could have been established using a Client Mobile IPv6 or any of its extensions, e.g. Proxy Mobile IPv6 signaling. The proposed revocation mechanism uses the Mobile IPv6 Generic Signalling Message framework as defined in [ID-MGSM] which has a generic message framework which is applicable to Mobile IPv6 [RFC3775] and Proxy Mobile IPv6 [ID-PMIP6] and can be used by any two IP mobility entities. As an example, this mechanism allows a local mobility agent, involved in providing IP mobility services to a mobile node, to notify the mobility access gateway of the termination of a mobile node binding registration. In another example, a mobility access gateway can use this mechanism to notify its local mobility anchor peer with a bulk termination of all Proxy MIPv6 bindings that are registered with the local mobility anchor and currently being served by the mobility access gateway.

2. Conventions & Terminology

2.1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.2. Terminology

All the general mobility related terminology and abbreviations are to be interpreted as defined in Mobile IPv6 specification [RFC3775] and Proxy Mobile IPv6 specification [ID-PMIP6].

3. Binding Revocation Protocol and Use Cases Overview

This specification defines a binding revocation mechanism using the framework of Mobile IPv6 Generic Signaling Message (MGSM), where a mobility node can communicate to the mobile node or another mobility node the termination of the mobile node registration binding. The following subsections describe the protocol overview and applicable

use cases.

3.1. Binding Revocation Protocol

In the case of Client Mobile IPv6, the revocation procedure can be initiated by the home agent. If the home network decides to terminate the service of the mobile node, the home agent sends a Binding Revocation Indication (BRI) message to the mobile node. The home agent includes the HoA option as specified in [RFC3775] to indicate the impacted mobile node session. When the mobile node receives a BRI message with its HoA included and the Acknowledge (A) bit is set, the mobile node responds by sending a Binding Revocation Acknowledgement (BRA) message.

In the case of DSMIPv6 [ID-DSMIP6], the revocation procedure can also be initiated by the home agent. If the home network decides to terminate the service of the mobile node, the home agent sends a BRI message to the mobile node to indicate the termination the mobile node IP Mobility service. The home agent may include the HoA option with the mobile node assigned home IPv4 address. After receiving the BRI message with the Acknowledge (A) bit is set, the mobile node responds by sending a BRA message.

Similarly, in the case of Proxy Mobile IPv6 [ID-PMIP6], the revocation procedure can be initiated by the local mobility anchor by sending a BRI message to communicate the termination of a mobile node registration binding to the mobility access gateway. In this case, the local mobility anchor includes the mobile node Home Network Prefix option [ID-PMIP6] and the MN-ID option [RFC4283] to indicate to the mobility access gateway the identity of the PMIPv6 binding that needs to be terminated. When the mobility access gateway receives the BRI message with the (A) bit set, the mobility access gateway responds to the local mobility anchor by sending a BRA message.

On the other hand, the mobility access gateway usually sends a de-registration message by sending a Proxy BU with a lifetime of zero to indicate to the local mobility anchor of the termination of the PMIPv6 mobile node binding registration. In this case, the mobility access gateway include the MN home network prefix option and the MN-ID option as per [ID-PMIP6] in order for the local mobility anchor to identify the mobile node PMIPv6 binding. However, in the case when the mobility access gateway communicates a bulk termination of PMIPv6 sessions, the mobility access gateway sends a BRI message with the G bit set and includes the mobility access gateway identity in the MN-ID option. When the local mobility anchor receives such BRI message, it ensures that the mobility access gateway is authorized to send such bulk termination message and then process the BRI message

accordingly. If the local mobility anchor processes the BRI message successfully and the (A) bit is set in the BRI, the local mobility anchor responds to the mobile access gateway by sending a BRA message. Additionally, the initiator of the binding revocation procedure include an indication in the Revocation Trigger field to indicate to the receiving node the cause for the revocation procedure.

3.2. Client MIPv6 and DSMIP6 Use Case

Binding revocation mechanism is applicable to Client Mobile IPv6 and DSMIPv6 session when the home agent needs to inform the mobile node that its binding registration has been revoked, e.g. for an administrative reason. This mechanism enables the home domain to dynamically allow the user to act upon the revocation message in order to not have an unexpectedly interrupted mobile IPv6 services.

In this case, the home agent sends a BRI message to indicate to the mobile node that its current mobile IPv6 binding has been revoked and it no longer can receive IP mobility service. The home agent includes the mobile node home address in HoA option, in the destination option header as used in [RFC3775] and sets the Revocation Trigger field to a proper value, e.g. Administrative. In the case of DSMIPv6 session, the home agent may additionally include the mobile node assigned IPv4 Home Address Option . When the mobile node receives the BRI message, it sends a BRA message as described in Section 10.2 to the home agent. Figure 1 illustrates the message sequencing when home agent revokes a mobile node binding registration.

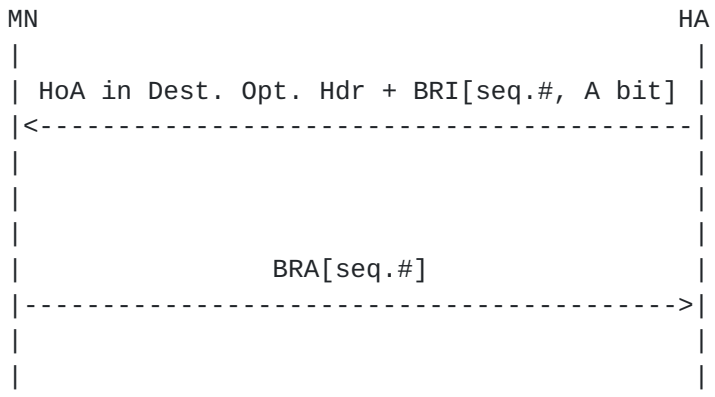


Figure 1: Home Agent Revokes a Mobile Node Binding Registration

3.3. Multi-Care of Addresses (Monami6) Use Case

In the case of Monami6 protocol, a mobile node is able to register multiple care-of addresses for the same home address [ID-MCoA]. Binding revocation mechanism is applicable to Monami6 when the home agent sends a BRI message to revoke a single or more care-of address bindings.

3.3.1. Termination of Multiple Care-of Addresses Bindings

In the case of multiple care-of addresses, the home agent maintains different binding for each pair of care-of address and home address. These bindings are also indexed and identified during the mobile node registration using a new Binding ID mobility option [ID-MCoA]. In this case, the home agent may revoke any binding, more than one binding, or all of the bindings for the same mobile node home address.

In the case when home agent revokes a single binding for a mobile node with multiple care-of addresses registration, the home agent send a BRI message to the mobile node with the corresponding BID option included and the HoA option in the destination option header. If the home agent needs to revoke more than one of the mobile node registered care-of addresses, the home agent includes all the corresponding BID options which reference these care-of addresses in the same BRI message. Figure 2 illustrates the message flow when the home agent revokes two registered Care-of addresses for the same MN in a single BRI message. The home agent can revoke any registered bindings by sending a BRI message to the respective mobile node.

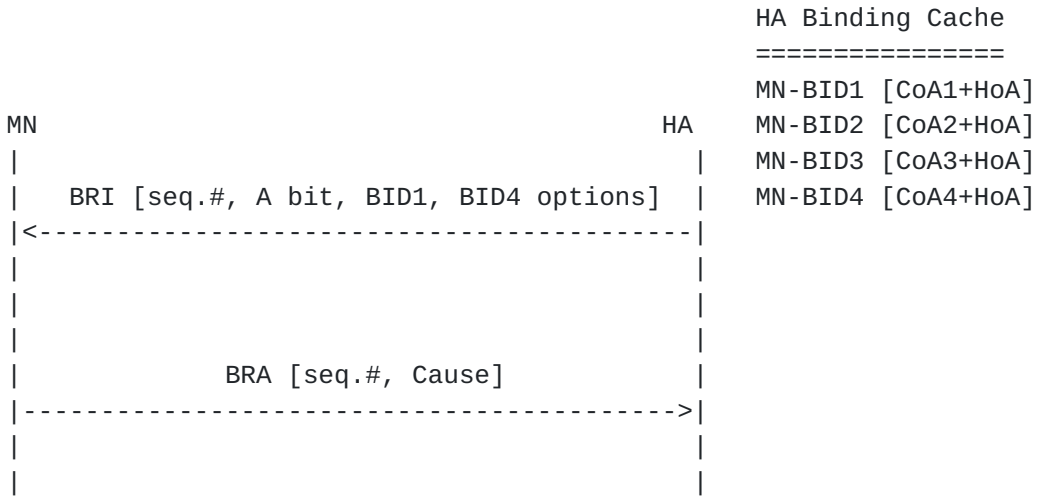


Figure 2: Home Agent Revokes MN's Specific Care-of Addresses Bindings

3.3.2. Termination of All Care-of Addresses Bindings

The home agent may revoke all of the mobile node registered bindings, by sending a BRI message without including any BID options while the HoA option is included in the destination options header. Figure 1 illustrates the message flow when the home agent revokes all registered Care-of addresses bindings for a MN in a single BRI message.

3.4. Proxy MIPv6 Use Case

Since the Mobile node does not participate in the mobility mechanism in the case of PMIPv6, there are many scenarios where Binding Revocation mechanism is needed to clean resources and make sure that the mobility entities, e.g. MAG and LMA, are always synchronized with the status of the existing proxy mobile IPv6 bindings. The binding revocation mechanism is generic enough that can be used in all applicable PMIPv6 scenarios and deployment options. For example, this revocation mechanism is still applicable and can be used when PMIPv6 is deployed with IPv6 or IPv4 transports and when the mobile node uses IPv4 or IPv6 address as specified in [ID-PMIP6-IPv4].

When the mobile access gateway receives a BRI message as in Section 9.1.1, the mobile access gateway sends a BRA message to the local mobility anchor following the rules describes in Section 9.1.2. Similarly if the local mobility anchor receives a BRI message with the A bit is set, the local mobility anchor responds to the mobile access gateway by sending a BRA message.

3.4.1. Local Mobility Anchor Revokes A PMIPv6 Binding

The local mobility anchor may send a BRI message to the mobile access gateway, hosting a specific proxy mobile IPv6 session, with the appropriate value in the revocation trigger field to indicate that the mobile node binding has been terminated and the mobile access gateway can clean up the applicable resources. When the mobile access gateway receives a BRI message, the MAG identify the respected binding and if the A bit was set in the received BRI message, the MAG sends a BRA message to the LMA. In this case, the MAG could send a Router Advertisement message to the MN with the home network prefix lifetime is set to zero.

As an example, Figure 3, illustrates the message sequence for revoking a mobile node binding at the source MAG during the MN inter-MAG handoff. During the inter-MAG handoff, the mobile node moves from the source MAG to the target MAG. The target MAG sends a PBU with the new care-of-address to the LMA to update the mobile node point of attachment. Since the MN binding at the LMA points to the source MAG and upon receiving the PBU from the target MAG, LMA updates the MN BCE and send a PBA to the target MAG. LMA can send a BRI message with the appropriate revocation trigger value, e.g. inter-MAG handoff indication, to the source MAG in order to clean up the applicable resources reserved for the specified MN. The MAG acknowledges the BRI message by sending a BRA message to indicate the success or failure of the termination of the mobile node binding.

The process identified above can also be used by the LMA in scenarios other than the inter-MAG handoff with the proper revocation trigger value to indicate to the peer MAG that a specific proxy mobile IPv6 binding or bindings have been revoked.

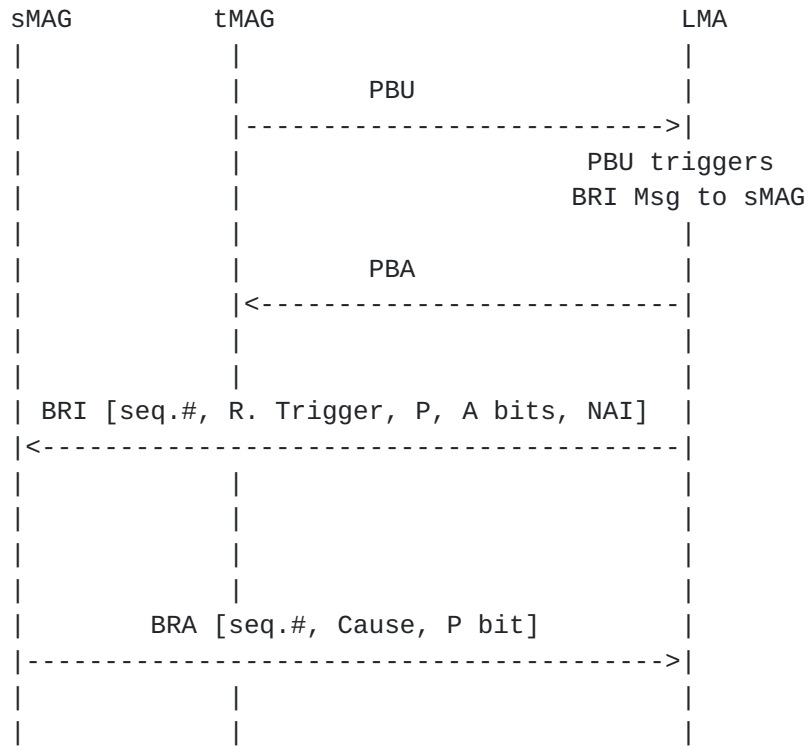


Figure 3: LMA Revokes a MN Registration During Inter-MAG Handoff

3.4.2. Local Mobility Anchor Revokes Bulk PMIPv6 Bindings

The local mobility anchor sends a BRI message to indicate that all bindings which are hosted by the peer mobile access gateway and registered with the local mobility anchor are being revoked by setting the G bit as described in Section 8.1.1.

3.4.3. Mobile Access Gateway Revoke Bulk PMIPv6 Bindings

The mobile access gateway sends a BRI message with the G bit is set to indicate that all mobility sessions which are registered at the LMA and attached to the MAG are being revoked as in Section 9.2.1. When the LMA receives a BRI message with the G bit is set from a specified MAG, the LMA checks if the MAG is authorized to use global revocations and responds with the appropriate status code by sending a BRA message as in Section 8.2.2.

4. Security Model

The revocation protocol described here requires the revocation messages to be defined as subtypes of the Mobile IPv6 Generic Signalling Message which is assigned a MH type value <IANA-TBD> [ID-MGSM] that requires IPsec protection. This is needed in order when IPsec is used for securing the mobility signalling between , e.g., the MAG and the LMA, the IPsec SPD will allow all MGSM packets including those which carry binding revocation messages.

Additionally, in the case when the LMA receives a BRI which indicates a bulk termination, the LMA MUST verify that the MAG sending the revocation indication message is authorized for Per-Peer Global revocation.

5. Binding Revocation Messages

This section defines two messages by reserving two subtypes of the Mobile IPv6 Generic Signalling Message that use the MH type which requires IPsec protection as defined in [ID-MGSM].

5.1. Binding Revocation Indication Message

The Binding Revocation Indication (BRI) message is used by the revoking mobility node to inform the receiving mobility entity that the IP mobility service of a specific binding or bindings have been revoked. Binding Revocation Indication message is sent as described

in Section 7.1, Section 8.1.1, and Section 9.2.1.

The Binding Revocation Indication (BRI) message uses the subtype <IANA-SUB1> of the MGSM message that use the MH type which requires IPsec protection as in [ID-MGSM]. When this subtype is indicated in the subtype field of the MGSM, the format of the Message Data field in the MGSM message following the subtype field is as in Figure 4

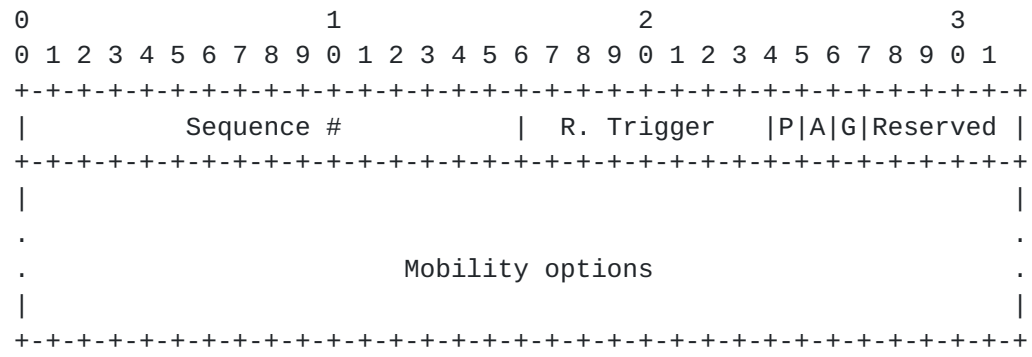


Figure 4: Binding Revocation Indication Message

Sequence #

A 16-bit unsigned integer used by the sending mobility node to match a returned Binding Revocation Acknowledgement with this Binding Revocation Indication.

Revocation Trigger

8-bit unsigned integer indicting the event which triggered the revoking node to send the BRI message. The following Revocation Trigger values are currently defined:

0 Reserved.
1 Unspecified.
2 Administrative Reason.
3 Inter-MAG Handover over same Access Types.
4 Inter-MAG Handover over different Access Types.
5 Per-Peer Policy.
6 Local Policy.

Proxy Binding (P)

The Proxy Binding (P) bit is set by the sending mobility node to indicate that the revoked binding is a proxy MIPv6 binding.

Acknowledge (A)

The Acknowledge (A) bit is set by the sending mobility node, e.g. LMA, HA, or MAG, to request a Binding Revocation Acknowledgement be returned upon receipt of the Binding Revocation Indication as in Section 7.1, Section 8.1.1, and Section 9.2.1.

Global (G)

The Global (G) bit is set by the sending mobility node, LMA or MAG, to request the termination of all Per-Peer mobility Bindings that are served by the sending and receiving mobility entities as in Section 8.1.1 and Section 9.2.1.

Reserved

These fields are unused. They MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. This document does not define any new mobility option. The receiver MUST ignore and skip any options which it does not understand. These mobility option(s) are used by the receiving mobility entity to identify the specific binding or bindings that the sending mobility entity requesting to be revoked.

The following options are valid in a Binding Revocation Indication:

- Home Network Prefix option [ID-PMIP6]. This option is mandatory when the P bit is set.

- Mobile Node Identifier Option [RFC4283]. This option is mandatory when the P bit is set. Additionally, If the G bit is set by the mobile access gateway, this option include the MAG identity.

- Binding ID mobility option [ID-MCoA]. This option is mandatory if the sending mobility entity request to terminate one binding of a multi care-of addresses bindings for the same mobile node. The sending Mobility entity may include more than one of these

mobility options.

- o IPv4 Home Address option which contains the mobile node home IPv4 address [ID-DSMIP6].

If no options are present in this message, 4 octets of padding are necessary and the Header Len field of the MGSM will be set to 1.

5.2. Binding Revocation Acknowledgement Message

The Binding Revocation Acknowledgement is used to acknowledge receipt of a Binding Revocation Indication described in Section 5.1. This packet is sent as described in Section 8.2.2, Section 9.1.2, and Section 10.2.

The Binding Revocation Acknowledgement uses the subtype <IANA-SUB2> of the MGSM message that use the MH type which requires IPsec protection as in [ID-MGSM]. When this subtype is indicated in the subtype field of the MGSM, the format of the Message Data field in the MGSM message following the subtype field is as in Figure 5:

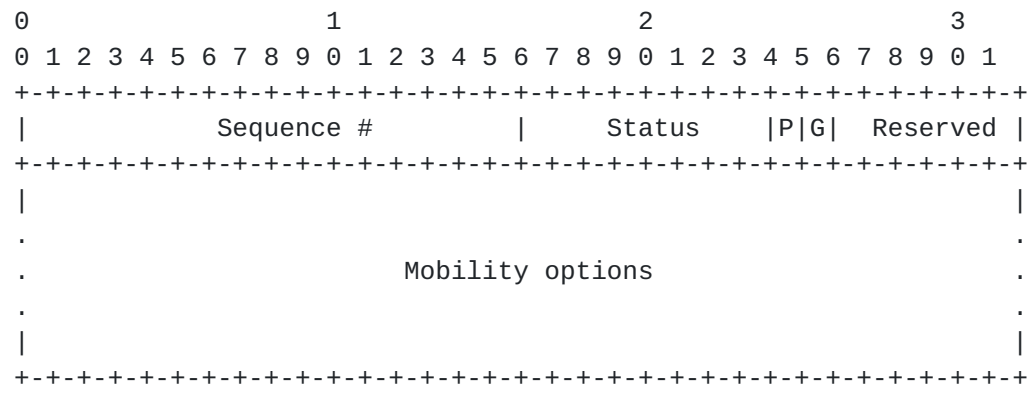


Figure 5: Binding Revocation Acknowledgement Message

Sequence #

The sequence number in the Binding Revocation Acknowledgement is copied from the Sequence Number field in the Binding Revocation Indication. It is used by the revoking mobility entity, e.g. HA, LMA, in matching this Binding Revocation Acknowledgement with the outstanding BRI.

Status

8-bit unsigned integer indicating the result of processing the Binding Revocation Indication message by the receiving mobility entity. The following status values are currently defined.

0 success.
1 partial success.
2 Binding Does NOT Exist.
3 Global Revocation NOT Authorized.
4 CAN NOT Identify Binding.

Proxy Binding (P)

The Proxy Binding (P) bit is set if the (P) bit is set in the corresponding Binding Revocation Indication message.

Global (G)

The Global (G) bit is set if the (G) bit is set in the corresponding BRI message. Section 8.2.2 and Section 9.1.2.

Reserved

These fields are unused. They MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Mobility Options

Variable-length field of such length that the complete Mobility Header is an integer multiple of 8 octets long. This field contains zero or more TLV-encoded mobility options. In the case when the Status field is set to success, no mobility option is required. The mobility option(s) is usually used to communicate information of the bindings that failed the revocation procedure.

The following options are valid in a Binding Revocation Acknowledgement:

- Home Network Prefix option [ID-PMIP6]. This option is mandatory when the P bit is set.

- Mobile Node Identifier Option [RFC4283]. This option SHOULD be included if the Home Network Prefix option is included.

- Binding ID mobility option [ID-MCoA]. This option MAY be included to indicate the specific Binding ID that the receiving node failed to revoke.

If no options are present in this message, 4 octets of padding are necessary and the Header Len field of the MGSM will be set to 1.

6. Binding Revocation Process Considerations

The following subsections describe the details of the binding revocation generic process by the different mobility entities.

6.1. Sending Binding Revocation Messages

When sending a Binding Revocation message, the sending mobility node, initiator, follows the rules of constructing a MGSM as in [ID-MGSM] and by setting the subtype field to a value <IANA-SUB1> to indicate a BRI message.

The mobility entity which initiates the revocation process, initiator, MUST use the underlying IPsec security association as described in [ID-MGSM] to secure the BRI and BRA messages transmission with the responding mobility entity, responder.

When a mobility entity initiate the binding revocation process by sending a Binding Revocation Indication, the initiator MUST construct the BRI message as described in Section 5.1. In the BRI message, the initiator MUST set the Sequence Number field to the next sequence number available for Binding Revocation. Since sending Binding Revocation Indication messages is not done on a regular basis, a 16 bit sequence number field is large enough to allow the initiator to match the Binding Revocation Acknowledgement to the outstanding Binding Revocation Indication with (A) bit set using the sequence number field only.

On the other hand, when the responder acknowledge the BRI message by sending a BRA, the responder follows the rules of constructing a MGSM as in [ID-MGSM] and by setting the subtype field to a value <IANA-SUB12> to indicate a BRA message and MUST construct the Binding Revocation Acknowledgement as described in Section 5.2. In this case, the responder MUST set the Sequence Number field by copying the value from the Sequence Number field of the received Binding Revocation Indication. Additionally, it MUST set the status field to a valid value that reflects the processing of the received Binding Revocation Indication.

6.2. Receiving Binding Revocation Messages

When receiving a Binding Revocation message, the receiving mobility node MUST verify the Mobile IPv6 Generic Signaling Message as in [ID-MGSM]. If the packet is dropped due to the receiving node does

not support Binding Revocation Indication as a MGSM with subtype <IANA-SUB1>, it MUST follow the processing rules as in [ID-MGSM] and it MUST send a Binding Error message with the Status field set to 2 (unrecognized MH Type value).

Since some mobility entities, e.g. LMA and MAG, are allowed to receive and possibly send a BRI or a BRA for different cases, IPsec mechanism will prevent any possible man in the middle reflection attack.

Upon receiving a packet carrying a Binding Revocation Indication, the receiving mobility entity, responder, validates that the packet was received protected with the underlying IPsec protection with the responding mobility entity as described in [ID-MGSM].

Upon receiving a packet carrying a Binding Revocation Acknowledgement, the receiving mobility entity, initiator, MUST validate that Sequence Number field matches the Sequence Number of an outstanding Binding Revocation Indication that was sent by the initiator. If the Sequence Number does not match any sequence number of any of the outstanding BRI, the receiving node MUST ignore the message but MAY log the event.

6.3. Retransmission of Binding Revocation Indication

If the sending mobility entity does not receive a Binding Revocation Acknowledgement in response to the outstanding Binding Revocation Indication before the MINDelayBRIs timer expires, the mobility entity, e.g. LMA, may retransmit the same BRI message up to the BRIMaxRetriesNumber as defined in Section 11. If the revoking mobility entity does not receive a BRA message after the maximum number of retransmits have been sent, the revoking mobility entity can clean the mobile node binding cache and all resources associated with this binding. The revoking mobility entity may log the event.

7. Home Agent Operation

7.1. Sending Binding Revocation Indication

When an event requires the home agent to terminate a mobile node mobile IPv6 registration, e.g. for administrative reason, the home agent sends a Binding Revocation Indication message to the mobile node to inform the mobile node that its specified binding has been revoked and it will no longer be able to receive an IP connectivity via its binding with the home agent.

To terminate a mobile node registration and its current binding with

the home agent, the home agent sends a packet to the mobile node containing a Binding Revocation Indication, with the packet constructed as follows:

- The Acknowledge (A) bit MAY be set in the Binding Revocation Indication to request the mobile node to send a Binding Revocation Acknowledgement upon receipt of the BRI.

- The Revocation Trigger field MUST be set in the Binding Revocation Indication to indicate to the mobile node the reason for revoking its IP mobility binding with the home agent. The Revocation Trigger may be used by the mobile node to take further steps if necessary.

- The packet MUST contain a Home Address destination option, which contains the mobile node's registered home address for the binding being revoked.

- The care-of address for the binding MUST be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Revocation Indication.

- The packet MAY contain a Home Address option which contains the mobile node's registered IPv4 home address for the binding being revoked.

The Acknowledge (A) bit in the Binding Revocation Indication requests the mobile node to return a Binding Revocation Acknowledgement in response to this Binding Revocation Indication. As described in Section 6.3, the home agent SHOULD retransmit this Binding Revocation Indication to the mobile node before terminating its IP connection until it receives a matching Binding Revocation Acknowledgement or the BRIMaxRetransmitNumber has been reached.

When the home agent send a Binding Revocation Indication to the mobile node, the home agent sets a flag in the mobile node BCE to indicate that revocation is in progress and starts the MINDelayBRIs timer. The home agent maintain the mobile node BCE in this state until it receives a Binding Revocation Acknowledgement or the BRIMaxRetransmitNumber is reached.

When the home agent needs to revoke one or more of a mobile node bindings that were created using Multi Care-of address registration as in [ID-MCoA], the home agent MUST include all the related Binding ID options that identify these bindings. In the case when the home agent needs to revoke all of the mobile node bindings, the home agent

MUST use the mobile node home address in the Home Address destination option and MUST NOT include any Binding ID option.

The home agent MUST use the IPsec security association as described in [ID-MGSM] to secure the MGSM that carries the BRI and BRA messages transmission with the mobile node.

7.2. Receiving Binding Revocation Acknowledgement

When the home agent receives a packet carrying a valid Binding Revocation Acknowledgement that was successfully processed as in Section 6.2, the home SHOULD examine the Status field as follows:

- If the Status field indicates that the Binding Revocation Indication was processed successfully, the home agent delete the MINDelayBRIs timer and the mobile node bindings and all related resources.

- If the Status field indicates any value other than success, the home agent SHOULD examine any mobility options included in the Binding Revocation Acknowledgement. The home agent MAY log the appropriate event to reflect the status of the received BRA.

8. Local Mobility Anchor Operation

8.1. Binding Revocation Initiator

8.1.1. Sending Binding Revocation Indication

When an event requires the local mobility agent to terminate a mobile node proxy mobile IPv6 registration, e.g. for administrative reason or inter-MAG handover, the local mobility agent sends a Binding Revocation Indication message to the mobile access gateway which host the mobile node proxy CoA to indicate that the mobile node specified binding should be removed. It also indicate that the local mobility anchor will no longer maintain a tunnel for this mobile node binding which points to the mobile node proxy CoA that is hosted at this mobile access gateway.

To terminate a mobile node proxy mobile IPv6 registration and its current PMIPv6 binding with the local mobility agent, the local mobility agent sends a packet to the mobile access gateway containing a Binding Revocation Indication following the procedure in Section 6.1 and the following rules:

- The Acknowledge (A) bit MAY be set in the Binding Revocation Indication to request the mobile access gateway to send a Binding Revocation Acknowledgement upon receipt of the BRI.

- The Proxy Mobile IP (P) bit MUST be set in the Binding Revocation Indication to indicate that the binding being revoked is a proxy Mobile IPv6 binding.

- The Revocation Trigger field MUST be set in the Binding Revocation Indication to indicate to the mobile access gateway the reason for removing the specified mobile node proxy mobile IPv6 binding at the local mobility anchor. The Revocation Trigger may be used by the mobile access gateway node to learn the mobile node latest movement.

- The Global (G) bit MUST be set and the Revocation Trigger MUST contain a value of Per-Peer Policy in the Binding Revocation Indication to request the mobile access gateway to remove all Per-Peer bindings that are registered with the local mobility anchor and hosted at this mobile access gateway.

- Whenever the Global (G) bit is set in the BRI, the Acknowledge (A) bit MUST be set to request the mobile access gateway to send a Binding Revocation Acknowledgement upon receipt of the BRI.

- The packet MUST contain the Mobile Node Identifier, MN-ID, option which contains the mobile node's NAI that was used in the Binding Update during the mobile node registration.

- The packet MUST contain a Home Network Prefix option, which contains the mobile node's registered Home Network Prefix for the binding being revoked.

- The care-of address for the binding MAY be used as the Source Address in the packet's IPv6 header, unless an Alternate Care-of Address mobility option is included in the Binding Revocation Indication.

The Acknowledge (A) bit in the Binding Revocation Indication requests the mobile access gateway to return a Binding Revocation Acknowledgement in response to this Binding Revocation Indication. As described in Section 6.3, the local mobility anchor SHOULD retransmit this Binding Revocation Indication to the mobile access gateway before deleting the mobile node IP tunnel to the mobile access gateway until it receives a matching Binding Revocation Acknowledgement or the BRIMaxRetransmitNumber is reached. The local mobility anchor MAY delete the mobile node(s) IP tunnel immediately

after sending the Binding Revocation Indication before receiving the BRA message.

When the local mobility anchor send a Binding Revocation Indication to the mobile access gateway to remove a specific binding, the local mobility anchor sets a flag in the mobile node proxy BCE to indicate that revocation is in progress and starts the MINDelayBRIs timer. The local mobility anchor SHOULD maintain the mobile node proxy BCE in this state until it receives a Binding Revocation Acknowledgement or the BRIMaxRetransmitNumber is reached. In the case when the local mobility anchor sets the Revocation Trigger field to a value which indicate inter-MAG handover, the local mobility anchor MAY switch the mobile node IP tunnel to the target mobile access gateway before sending a Binding Revocation Indication to the sources mobile access gateway.

When the local mobility anchor needs to revoke all mobile nodes proxy BCE that are registered with the local mobility anchor and hosted at the mobile access gateway, the local mobility anchor MUST set the Global (G) bit and the value of the Revocation Trigger field to Per-Peer Policy. In this case, the local mobility anchor MUST NOT include any mobility options in the Binding Revocation Indication.

When the local mobility anchor needs to revoke all mobile nodes proxy BCE that belong to a specific realm, e.g. @companyabc.com, and are registered with the local mobility anchor and hosted at the mobile access gateway, the local mobility anchor MUST set the Global (G) bit and the value of the Revocation Trigger field to Local Policy. In this case, the local mobility anchor MUST include a mobility option to identify the impacted bindings, e.g. MN-ID option with a wildcard NAI, e.g. *@companyabc.com, to identify all the mobile nodes BCEs that need to be removed.

When the mobile node is registered with multiple Home Network Prefixes for the same proxy care-of address, the local mobility anchor SHOULD include a Home Network Prefix option for each registered Home Network Prefix in the Binding Revocation Indication. Alternatively, the local mobility anchor MAY include only the mobile node identifier, MN-ID, option in the Binding Revocation Indication to indicate to the mobile access gateway to remove all bindings of the specified mobile node NAI in the MN-ID option.

8.1.2. Receiving Binding Revocation Acknowledgement

When the local mobility anchor receives a packet carrying a valid Binding Revocation Acknowledgement that was successfully processed as in Section 6.2 and if the mobile node BCE is in the state of Revocation in progress, the local mobility anchor SHOULD examine the

Status field before clearing the mobile node related resources as follows:

- If the Status field indicates that the Binding Revocation Indication was processed successfully, the local mobility anchor delete the MINDelayBRIs timer and the mobile node proxy bindings and all associated resources.

- If the Status field indicates partial success value or MN binding does not exist, the local mobility anchor SHOULD examine mobility options that included in the Binding Revocation Acknowledgement, if any, before deleting the MINDelayBRIs timer and the mobile node associated proxy bindings and all related resources. It is based on the local mobility anchor local policy how to handle the Mobile node BCE that the mobile access gateway indicated it failed the revocation procedure, however, the LMA MAY log the event.

8.2. Binding Revocation Responder

8.2.1. Receiving Binding Revocation Indication

When the local mobility anchor receives a packet carrying a Binding Revocation Indication that was successfully processed as in Section 6.2, the local mobility anchor SHOULD in addition process the message as follows:

- Binding Revocation Indication is formatted as in Section 5.1 and if the (P) bit is set, the local mobility anchor must validate that all the impacted bindings MUST have the proxy binding flag set.

- If the Global (G) bit is set, the Binding Revocation Indication SHOULD contain the mobile access gateway ID in the MN-ID option. The local mobility anchor MUST verify that the identified mobile access gateway as per the value in the MN-ID option is authorized to use the Per-Peer Global bindings revocation. The mechanism the local mobility anchor use to verify the mobile access gateway authorization is out of scope of this document. When the (P) bit is set, this Binding Revocation Indication impact only the mobile nodes bindings that have the Proxy Mobile IP flag set.

- The local mobility anchor identify all impacted mobile nodes bindings and if the Acknowledgement (A) bit is set, the local mobility anchor MUST send a Binding Revocation Acknowledgement following Section 8.2.2 using the appropriate status code.

- If the Global (G) bit is not set, the local mobility anchor MUST use the included mobility options to identify the impacted mobile node binding as follows:

  1. If only the mobile node identifier, MN-ID, option is included, the local mobility anchor MUST revoke all bindings for this mobile node which have a proxy CoA that is hosted at the mobile access gateway that sent the BRI.

  2. If the mobile node identifier, MN-ID, and the Home Network Prefix option are included, the local mobility anchor MUST only remove the specified proxy binding.

  3. If the mobile node identifier, MN-ID, option and more than one Home Network Prefix options are included, the local mobility anchor need to remove the mobile node bindings which are referenced in these multiple Home Network Prefixes for the specified mobile node NAI.

The Revocation Trigger field value in the received Binding Revocation Indication could be used by the local mobility anchor to log an event or update some local parameters which tracks the state of the peer mobile access gateway.

8.2.2. Sending Binding Revocation Acknowledgement

When the local mobility anchor receive a valid Binding Revocation Indication with the (A) bit is set and after processing the BRI message, the local mobility anchor sends a packet to the mobile access gateway containing a Binding Revocation Acknowledgement following the process in Section 6.1 and the following:

- If the (P) bit was set in the received Binding Revocation Indication, the local mobility anchor MUST set the (P) bit in the Binding Revocation Acknowledgement.

- If the Global (G) bit was set in the received BRI, the local mobility anchor MUST set the (G) bit in the Binding Revocation Acknowledgement.

- The local mobility anchor MUST set the status field to a valid code that reflects the processing of the received Binding Revocation Indication. If the mobile access gateway is not authorized to use the Per-Peer Global revocation feature, the LMA MUST set the status field to (Global Revocation NOT Authorized).

- The local mobility MAY set the status field to partial success and in this case it MAY include the mobile node identifier or the Home Network Prefix option to identify the bindings that failed revocation.

- The destination IP address of the IPv6 packet of the Binding Revocation Acknowledgement is set to the source IP address of the received Binding Revocation Indication.

9. Mobile Access Gateway Operation

9.1. Binding Revocation Responder

9.1.1. Receiving Binding Revocation Indication

Upon receiving a packet carrying a Binding Revocation Indication, the mobile access gateway MUST validate the packet according to Section 6.2 and the following:

- Binding Revocation Indication MUST be formatted as in Section 5.1 and if the (P) bit is set, the mobile access gateway must validate that the impacted binding have the proxy binding flag set.

- If the Acknowledgement (A) bit in the received BRI is set, the mobile access gateway MUST send a Binding Revocation Acknowledgement following Section 9.1.2 using the appropriate status value.

- If the Global (G) bit is set and the Revocation Trigger field is set to Per-Peer policy, the mobile access gateway identify all bindings that are registered at the local mobility anchor and hosted at the mobile access gateway. This Binding Revocation Indication does not include any other mobility options. However, if the (P) bit is set, this Binding Revocation Indication MUST only impact mobile nodes bindings that have the Proxy Mobile IP flag set.

- If the Global (G) bit is set and the Revocation Trigger field is set to Local policy, the mobile access gateway MUST identify all bindings that are registered at the local mobility anchor and hosted at the mobile access gateway using the mobility option included in the Binding Revocation Indication. This Binding Revocation SHOULD include at least the MN-ID option, e.g. with a wild card NAI.

- If the Global (G) bit is set and the Revocation Trigger field is set to Local policy, and no mobility options are included in the Binding Revocation Indication message, the mobile access gateway MUST treat this as an error scenario. In this case, the mobile access gateway SHOULD send a Binding Revocation Acknowledgement message with status "CAN NOT Identify Binding".

The Revocation Trigger field value in the received Binding Revocation Indication could be used by the mobile access gateway to define what actions the mobile access gateway could do to inform the mobile node that its IP connectivity to the current Home Network Prefix has been terminated. e.g. if the Revocation Trigger field is set to administrative value, the mobile access gateway may send a RA message after setting the Home Network Prefix lifetime to zero.

If the Revocation Trigger field value in the received Binding Revocation Indication message indicate an inter-MAG handover and the (A) bit is set, the mobile access gateway MAY validate that the mobile node is no longer attached to the mobile access gateway before sending a Binding Revocation Acknowledgement message to the local mobility anchor.

9.1.2. Sending Binding Revocation Acknowledgement

When the mobile access gateway receive a valid Binding Revocation Indication with the (A) bit is set and after processing the BRI message, the mobile access gateway sends a packet to the local mobility anchor containing a Binding Revocation Acknowledgement according to the procedure in Section 6.1 and the following:

- The mobile access gateway MUST set the (P) bit in the Binding Revocation Acknowledgement if it is set in the received BRI.

- If the Global (G) bit was set in the received BRI, the mobile access gateway MUST set the (G) bit in the Binding Revocation Acknowledgement.

- The mobile access gateway MUST set the status field to a valid code that reflects the processing of the received Binding Revocation Indication.

- The mobile access gateway MAY set the status field to partial success and in this case it MAY include the mobile node identifier, MN-ID, or the Home Network Prefix option to identify the binding(s) that failed to be removed as part of the revocation procedure.

- The destination IP address of the IPv6 packet of the Binding Revocation Acknowledgement is set to the source IP address of the received Binding Revocation Indication.

9.2. Binding Revocation Initiator

9.2.1. Sending Binding Revocation Indication

The mobile access gateway send a Binding Revocation Indication when it needs to use global revocation, i.e. when the G bit is set. In this case when an event occurs which requires the mobile access gateway to inform the local mobility anchor to terminate all mobile nodes bindings that are registered at the local mobility anchor and the mobile access gateway, the mobile access gateway send a Binding Revocation Indication message following Section 6.1 and the following:

- The Acknowledge (A) bit MUST be set in the Binding Revocation Indication to request the local mobility anchor to send a Binding Revocation Acknowledgement upon receipt of the BRI.

- The Proxy Mobile IP (P) bit MUST be set in the Binding Revocation Indication to indicate that bindings that being revoked is a proxy Mobile IPv6 binding.

- The Global (G) bit MUST be set and the Revocation Trigger MUST contain a value of Per-Peer Policy in the Binding Revocation Indication to request the local mobility anchor to remove all Per-Peer bindings that are registered with the local mobility anchor and hosted at this mobile access gateway. In this case, the mobile node identifier, MN-ID, option MUST be included in the BRI and MUST contain the mobile access gateway identity

- The mobile access gateway address MAY be used as the Source Address in the packet's IPv6 header.

The Acknowledge (A) bit in the Binding Revocation Indication requests the local mobility anchor to return a Binding Revocation Acknowledgement in response to this Binding Revocation Indication. As described in Section 6.3, the mobile access gateway SHOULD retransmit this Binding Revocation Indication to the local mobility anchor until it receives a matching Binding Revocation Acknowledgement or the BRIMaxRetransmitNumber is reached. The mobile access gateway MAY delete the mobile nodes IP tunnels immediately after sending the Binding Revocation Indication before receiving a BRA message from the LMA.

9.2.2. Receiving Binding Revocation Acknowledgement

When the mobile access gateway receive a packet carrying a valid Binding Revocation Acknowledgement that was successfully processed according to Section 6.2, the mobile access gateway MUST validate the BRA as per the followings:

- When the mobile access gateway receive a packet carrying a valid Binding Revocation Acknowledgement and the Global (G) and Proxy MIPv6 (P) bits are set and the mobile nodes BCEs are in the state of Revocation in Progress, the mobile access gateway SHOULD examine the Status field as follows:

- If the Status field indicates that the Binding Revocation Indication was processed successfully, the mobile access gateway delete the MINDelayBRIs timer and the mobile nodes proxy bindings and all associated resources.

- If the Status field indicates (Global Revocation NOT Authorized), the mobile access gateway is not authorized to participate in a Per-Peer Global Revocation. The mobile access gateway SHOULD NOT retry sending a Binding Revocation Indication with the Global (G) bit is set to the same local mobility agent. The mobile access gateway should raise an alarm or log an event to indicate this rejection.

10. Mobile Node Operation

10.1. Receiving Binding Revocation Indication

Upon receiving a packet carrying a Binding Revocation Indication, the mobile node MUST validate the packet according to Section 6.2 and the following tests:

- The mobile node MUST verify that the IP address in the Home Address option is its Home Address.

- If the Acknowledgement (A) bit is set in the Binding Revocation Indication and the MN has the BCE in registered state, the mobile node MUST send a Binding Revocation Acknowledgement. However, in all other cases when the (A) bit is set in the BRI, the mobile node SHOULD send a Binding Revocation Acknowledgement. In all cases, the mobile node MUST follow Section 10.2 when send a BRA using the appropriate status code.

- The mobile node MUST verify that the (P) bit in the Binding Revocation Indication is NOT set. If the (P) bit is set, the mobile node MUST silently discard the Binding Revocation Indication.

- If the Revocation Trigger field value is Administrative, the mobile node MUST not try to re-register with the home agent before contacting its home operator.

- If the mobile node has registered multiple care-of addresses with its home agent, the mobile node MUST verify which binding is being revoked by examining the content of the BRI message. If the mobile node received a Binding Revocation Indication with a single or more than one BID options and its home address is in the Home Address option, the mobile node MUST consider its bindings identified in the Binding ID options are being revoked.

- If the mobile node has multi Care-of Addresses bindings with its home agent and received a Binding Revocation Indication, with only its home address in the Home Address option, the mobile node MUST consider all of its registered care-of addresses bindings with this home address have been revoked.

The Revocation Trigger field value in the received Binding Revocation Indication could be used by the mobile node to define what action the mobile node could do to be able to register again and receive its IP mobility service, e.g. contacting its home operator.

10.2. Sending Binding Revocation Acknowledgement

When the mobile node receive a valid Binding Revocation Indication with the (A) bit is set from its home agent and while having this BCE in registered state, the mobile node MUST send a packet to its home agent containing a Binding Revocation Acknowledgement according to the procedure in Section 6.1 and the following:

- The mobile node MUST set the status field to successful to reflect that it has received the Binding Revocation Indication and acknowledge that its IP connectivity with its home agent has been revoked.

- The destination IP address of the IPv6 packet of the Binding Revocation Acknowledgement is set to the source IP address of the received Binding Revocation Indication.

- If the mobile node receive a Binding Revocation Indication from a home agent which the mobile node does not have a registered binding with, the mobile node SHOULD silently discard the BRI message. The mobile node should continue to use its assigned HoA to access its IP mobility service.

11. Protocol Configuration Variables

Any mobility entity which is allowed to invoke the binding revocation procedure by sending a Binding Revocation Indication message SHOULD allow the following variables to be configured.

BRI Maximum Number of Retries (BRIMaxRetriesNumber)

This variable specifies the maximum Number of times a mobility entity can retransmit a Binding Revocation Indication message before receiving a Binding Revocation Acknowledgement message. The default value for this parameter is 1.

Minimum Delay Between BRI messages (MINDelayBRIs)

This variable specifies the delay time in seconds before the revoking mobility entity retransmits a BRI message. The default is 1 second but not less than 0.5 seconds.

12. IANA Considerations

This document defines two new messages BRI and BRA, as described in Section 5.1 and Section 5.2 by using two subtypes of the Mobile IPv6 Generic Signalling Message which uses a MH type <TBD-IANA> as in [ID-MGSM] which requires the use of IPsec, The new subtype values <IANA-SUB1 and IANA-SUB2> needs to be assigned from the same numbering space as allocated for the other MGSM subtypes.

13. Security Considerations

The protocol described here uses the same security association between the MN and the HA or the MAG and the LMA that has been used to exchange the corresponding MIPv6 or Proxy MIPv6 BU and BA when the session was established. If IPsec is used, The SPD of this IPsec SA MUST allow the MH type for the MGSM.

However, in the case when the MAG sends a BRI message with the G bit is set, the LMA MUST verify that the MAG is authorized to use Per-Peer Global Revocation.

14. Acknowledgements

The authors would like to thank Ryuji Wakikawa, Bruno Mongazon-Cazavet and Domagoj Premec for their review and comments of this draft and all colleagues who have supported the advancement of this draft effort.

15. References

15.1. Normative References

[ID-DSMIP6] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", draft-ietf-mext-nemo-v4traversal-04 (work in progress), June 2008.

[ID-MCoA] Wakikawa, R., Devarapalli, V., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", draft-ietf-monami6-multiplecoa-08 (work in progress), May 2008.

[ID-MGSM] Haley, B. and S. Gundavelli, "Mobile IPv6 Generic Signaling Message", draft-haley-mext-generic-signaling-message-00 (work in progress), July 2008.

[ID-PMIP6] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", draft-ietf-netlmm-proxymip6-18 (work in progress), May 2008.

[ID-PMIP6-IPv4] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", draft-ietf-netlmm-pmip6-ipv4-support-03 (work in progress), May 2008.

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

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

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

15.2. Informative References

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

[RFC3543] Glass, S. and M. Chandra, "Registration Revocation in Mobile IPv4", RFC 3543, August 2003.

Authors' Addresses

Ahmad Muhanna
Nortel
2221 Lakeside Blvd.
Richardson, TX 75082
USA

Email: amuhanna@nortel.com

Mohamed Khalil
Nortel
2221 Lakeside Blvd.
Richardson, TX 75082
USA

Email: mkhalil@nortel.com

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

Email: sgundave@cisco.com

Kuntal Chowdhury
Starent Networks
30 International Place
Tewksbury, MA 01876
USA

Email: kchowdhury@starentnetworks.com

Parviz Yegani
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134
USA

Email: pyegani@cisco.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).