

Internet Engineering Task Force (IETF)
Request for Comments: 5846
Category: Standards Track
ISSN: 2070-1721

A. Muhanna
M. Khalil
Ericsson
S. Gundavelli
K. Chowdhury
Cisco
P. Yegani
Juniper Networks
June 2010

Binding Revocation for IPv6 Mobility

Abstract

This document defines a binding revocation mechanism to terminate a mobile node's mobility session and the associated resources. This mechanism can be used both with base Mobile IPv6 and its extensions, such as Proxy Mobile IPv6. The mechanism allows the mobility entity which initiates the revocation procedure to request its peer to terminate either one, multiple or all specified Binding Cache entries.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at <http://www.rfc-editor.org/info/rfc5846>.

Copyright Notice

Copyright (c) 2010 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 Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction	4
2. Conventions and Terminology	4
2.1. Conventions Used in This Document	4
2.2. Terminology	4
3. Binding Revocation Protocol and Use Cases Overview	5
3.1. Binding Revocation Protocol	5
3.2. MIPv6 and DSMIPv6 Use Case	6
3.3. Multiple Care-of Addresses (MCoA) Use Case	7
3.4. Proxy MIPv6 Use Case	8
3.4.1. Local Mobility Anchor Initiates PMIPv6 Revocation	9
3.4.2. Mobile Access Gateway Revokes Bulk PMIPv6 Bindings	10
4. Binding Revocation Messages over IPv4 Transport Network	10
5. Binding Revocation Message	11
5.1. Binding Revocation Indication Message	13
5.2. Binding Revocation Acknowledgement Message	16
6. Binding Revocation Process Operation	18
6.1. Sending Binding Revocation Message	18
6.1.1. Sending Binding Revocation Indication	18
6.1.2. Sending Binding Revocation Acknowledgement	19
6.2. Receiving Binding Revocation Message	20
6.2.1. Receiving Binding Revocation Indication	20
6.2.2. Receiving Binding Revocation Acknowledgement	21
6.3. Retransmission of Binding Revocation Indication	22
7. Home Agent Operation	22
8. Local Mobility Anchor Operation	23
8.1. Sending Binding Revocation Indication	23
8.2. Receiving Binding Revocation Indication	27
9. Mobile Access Gateway Operation	29
9.1. Receiving Binding Revocation Indication	29
9.2. Sending Binding Revocation Indication	31
10. Mobile Node Operation	32
11. Protocol Configuration Variables	34
12. IANA Considerations	34
13. Security Considerations	36
14. Acknowledgements	37
15. References	37
15.1. Normative References	37
15.2. Informative References	38

1. Introduction

In the case of Mobile IPv6 and for administrative reasons, 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 for its Home Address. A similar Mobile IPv4 registration revocation mechanism [RFC3543] has been specified by the IETF for providing a revocation mechanism for sessions that were established using Mobile IPv4 registration [RFC3344].

This document specifies a binding revocation mechanism that can be used to revoke a mobile node's mobility session(s). The same mechanism can be used to revoke bindings created using Mobile IPv6 [RFC3775] or any of its extensions, e.g., Proxy Mobile IPv6 [RFC5213]. The proposed revocation mechanism uses a new Mobility Header (MH) type 16 for revocation signaling that is applicable to Mobile IPv6 [RFC3775] and Proxy Mobile IPv6 [RFC5213] and can be used by any two IP mobility entities. As an example, this mechanism allows a local mobility anchor (LMA), involved in providing IP mobility services to a mobile node, to notify the mobile access gateway (MAG) of the termination of that mobile node binding registration. In another example, a mobile access gateway can use this mechanism to notify its local mobility anchor peer with a bulk termination of all or a subset of proxy mobile IPv6 (PMIPv6) bindings that are registered with the local mobility anchor and currently being served by the mobile access gateway. Any mobility entity is allowed to revoke only the registration of those mobile node(s) mobility sessions that are currently registered with it.

2. Conventions and 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 the Mobile IPv6 [RFC3775], Proxy Mobile IPv6 [RFC5213] and IPv4 Support for Proxy Mobile IPv6 [RFC5844] specifications. The following terms are used in this specification.

Initiator

The mobility node that initiates the binding revocation procedure by sending a Binding Revocation Indication message to its peer, e.g., home agent, local mobility anchor, or mobile access gateway.

Responder

The mobility node that receives the Binding Revocation Indication message and responds with a Binding Revocation Acknowledgement message, e.g., mobile node, mobile access gateway, or local mobility anchor.

3. Binding Revocation Protocol and Use Cases Overview

This specification specifies a generic binding revocation mechanism where a mobility node can communicate to the mobile node or another mobility node the identity of the mobile node registration binding that is being terminated. In the case when this mechanism is used for bulk termination or multiple bindings, the identities of these bindings are communicated to the mobile node or mobility node using the same generic mechanism. The following subsections present the protocol overview and applicable use cases.

3.1. Binding Revocation Protocol

In the case of Mobile IPv6, 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 home address (HoA) of the mobile node in the Type 2 routing header as specified in [RFC3775] to indicate the impacted mobile node binding. In the case of Dual Stack Mobile IPv6 (DSMIPv6) [RFC5555], the home agent may include the IPv4 Home Address option with the home IPv4 address assigned by the mobile node. Additionally, if the mobile node registered multiple care-of addresses [RFC5648], the home agent includes the Binding Identifier (BID) option(s) in the Binding Revocation Indication message to identify which binding is being revoked. When the mobile node receives a Binding Revocation Indication message with its HoA included in the Type 2 routing header, the mobile node responds by sending a Binding Revocation Acknowledgement (BRA) message.

Similarly, in the case of Proxy Mobile IPv6 [RFC5213], the revocation procedure can be initiated by the local mobility anchor by sending a Binding Revocation Indication message to communicate the termination of a mobile node registration binding to the mobile access gateway. In this case, the local mobility anchor includes the mobile node Home Network Prefix (MN-HNP) option [RFC5213] 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 mobile access gateway receives the Binding Revocation Indication message, the mobile access gateway responds to the local mobility anchor by sending a Binding Revocation Acknowledgement message.

On the other hand, the mobile access gateway usually sends a de-registration message by sending a Proxy Binding Update 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 mobile access gateway includes the MN-HNP option, the MN-ID option, and all other required mobility options as per [RFC5213] in order for the local mobility anchor to identify the mobile node PMIPv6 binding. Additionally, in the case when the mobile access gateway communicates a bulk termination of PMIPv6 mobility sessions, the mobile access gateway sends a Binding Revocation Indication message with the Global (G) bit set and includes the mobile access gateway identity in the MN-ID option, see Section 9.2 and Section 8.2. When the local mobility anchor receives such a Binding Revocation Indication message, it ensures that the mobile access gateway is authorized to send such a bulk termination message, see Section 13, and then processes the Binding Revocation Indication message accordingly. If the local mobility anchor processes the Binding Revocation Indication message successfully, the local mobility anchor responds to the mobile access gateway by sending Binding Revocation Acknowledgement message.

In any of the above cases, the initiator of the binding revocation procedure, e.g., home agent, local mobility anchor, or mobile access gateway, uses the Revocation Trigger field in the Binding Revocation Indication message to indicate to the receiving node the reason for initiating the revocation procedure.

3.2. MIPv6 and DSMIPv6 Use Case

The binding revocation mechanism is applicable to Mobile IPv6 and DSMIPv6 session(s) 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 user or the mobile node to react to the revocation, e.g., reinstate its interrupted Mobile IPv6 services.

In this case, the home agent sends a Binding Revocation Indication message to indicate to the mobile node that its current mobile IPv6 (MIPv6) binding has been revoked and it is no longer able to receive IP mobility service. The home agent includes the HoA in a Type 2 routing header as used in [RFC3775] and sets the Revocation Trigger field to a proper value, e.g., Administrative Reason. In the case of

a DSMIPv6 session, the home agent may additionally include the mobile-node-assigned IPv4 Home Address in the IPv4 Home Address option. When the mobile node receives the Binding Revocation Indication message, it sends a Binding Revocation Acknowledgement message to the home agent. Figure 1 illustrates the message sequencing when a home agent revokes a mobile node binding registration.

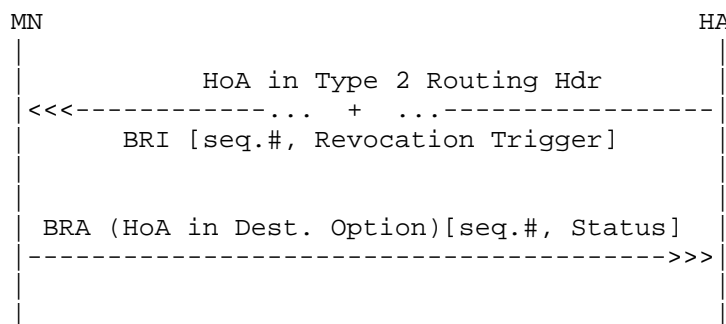


Figure 1: Home Agent Revokes a Mobile Node Binding Registration

3.3. Multiple Care-of Addresses (MCoA) Use Case

In the case of multiple care-of address registrations [RFC5648], the home agent maintains a different binding for each care-of address and home address pair. These bindings are also indexed and identified during the mobile node registration using a BID mobility option. The HA may revoke one or multiple bindings for the same mobile node home address.

If the home agent revokes a single binding for a mobile node with multiple care-of address registrations, the home agent sends a Binding Revocation Indication message to the mobile node with the corresponding BID option included. If more than one of the mobile node registered care-of addresses needs to be revoked, the home agent includes all the corresponding BID options in the same Binding Revocation Indication message. Figure 2 illustrates the message flow when the home agent revokes two registered care-of addresses for the same mobile node in a single Binding Revocation Indication message.

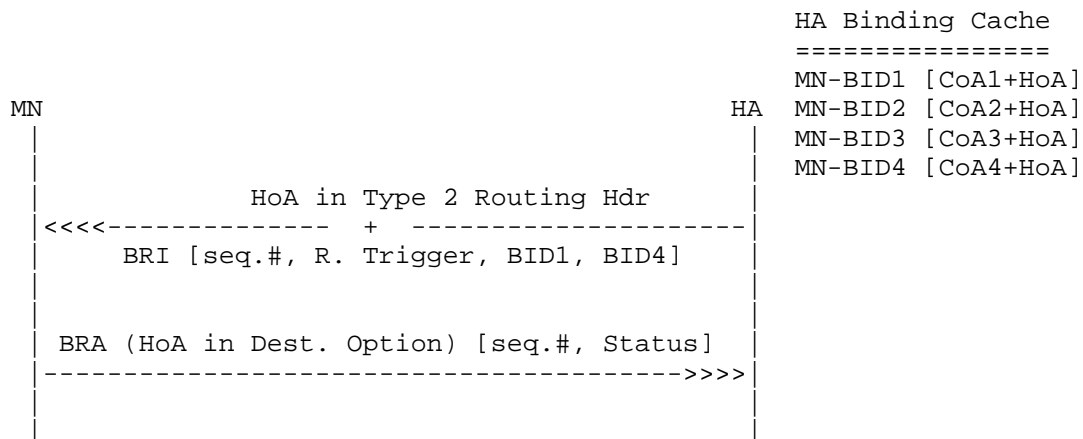


Figure 2: Home Agent Revokes MN's Specific Care-of Address Bindings

Additionally, 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 is included in the Type 2 routing header. Figure 1 illustrates the message flow when the home agent revokes all registered care-of address bindings for a mobile node in a single Binding Revocation Indication 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 the Binding Revocation mechanism is needed to clean resources and make sure that the mobility entities, i.e., mobile access gateway and local mobility anchor, are always synchronized with respect to the status of the existing PMIPv6 bindings. The binding revocation mechanism is generic enough that it can be used for all Proxy Mobile IPv6 scenarios that follow the [RFC5213] and [RFC5844] specifications.

When the mobile access gateway receives a Binding Revocation Indication message as in Section 9.1, the mobile access gateway sends a Binding Revocation Acknowledgement message to the local mobility anchor following the rules described in Section 6.1.2. Similarly, if the local mobility anchor receives a Binding Revocation Indication message, the local mobility anchor responds to the mobile access gateway by sending a Binding Revocation Acknowledgement message.

3.4.1. Local Mobility Anchor Initiates PMIPv6 Revocation

The local mobility anchor may send a Binding Revocation Indication message with the appropriate revocation trigger value to the mobile access gateway that hosts a specific PMIPv6 binding 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 Binding Revocation Indication message, the mobile access gateway identifies the respective binding and it sends a Binding Revocation Acknowledgement message to the local mobility anchor. In this case, the mobile access gateway could terminate the IPv6 or IPv4 mobility session on the access link and notify the mobile node as in Section 9.1.

As an example, Figure 3, illustrates the message sequence for revoking a mobile node binding at the source mobile access gateway during the mobile node inter-MAG handover. During the inter-MAG handover, the mobile node moves from the source MAG to the target MAG. The target MAG sends a Proxy Binding Update with the new care-of address to the local mobility anchor to update the mobile node's point of attachment. Since the mobile node binding at the local mobility anchor points to the source MAG and upon receiving the Proxy Binding Update from the target MAG, the local mobility anchor updates the MN Binding Cache entry (BCE) and sends a Proxy Binding Acknowledgement to the target MAG. The local mobility anchor can send a Binding Revocation Indication message with the appropriate revocation trigger value, e.g., inter-MAG handover - different Access Types, to the source MAG in order to clean up the applicable resources reserved for the specified mobile node binding. The source mobile access gateway acknowledges the Binding Revocation Indication message by sending a Binding Revocation Acknowledgement message to indicate the success or failure of the termination of the mobile node's binding.

The process identified above can also be used by the local mobility anchor in scenarios other than the inter-MAG handover with the proper revocation trigger value to indicate to the peer mobile access gateway that a specific PMIPv6 binding or bindings have been revoked.

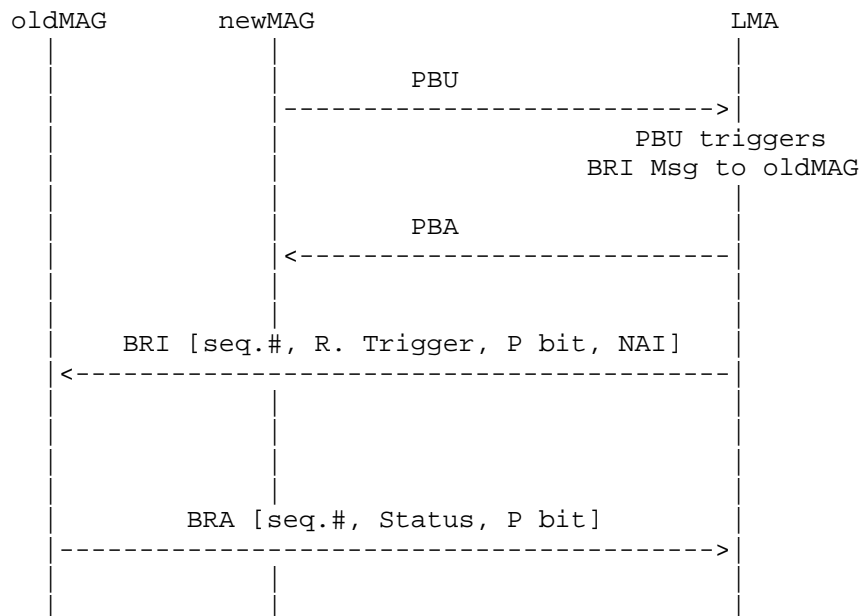


Figure 3: LMA Revokes an MN Registration During Inter-MAG Handover

In addition, the local mobility anchor can send a Binding Revocation Indication message to indicate that all bindings that are hosted by the peer mobile access gateway and registered with the local mobility anchor are being revoked by setting the Global (G) bit as described in Section 8.1.

3.4.2. Mobile Access Gateway Revokes Bulk PMIPv6 Bindings

The mobile access gateway sends a BRI message with the Global (G) bit set and the Revocation Trigger field set to "Per-Peer Policy" to indicate that all mobility bindings that are registered at the local mobility anchor and attached to the mobile access gateway are being revoked as in Section 9.2. When the local mobility anchor receives this Binding Revocation Indication message from the specified mobile access gateway, the local mobility anchor first checks if the mobile access gateway is authorized to use global revocations, then it responds with the appropriate status code by sending a Binding Revocation Acknowledgement message as in Section 6.1.2.

4. Binding Revocation Messages over IPv4 Transport Network

In some deployments, the network between the mobile access gateway and the local mobility anchor may only support IPv4 transport. Another case is when a mobile node that supports client mobile IPv6

roams to an access network where only IPv4 addressing and transport is supported. In this case, the mobile node is required to register an IPv4 home address with its home agent using a mobile IPv6 Binding Update message.

If the Proxy Binding Update and Proxy Binding Acknowledgement messages or the Binding Update and Binding Acknowledgement messages are sent using UDP encapsulation [RFC5844] [RFC5555], then the Binding Revocation Messages are sent using the same UDP encapsulation. The same UDP source and destination port numbers and IPv4 addresses used for exchanging the Proxy Binding Update and Proxy Binding Acknowledgement or the Binding Update and Binding Acknowledgement messages MUST be used when transporting Binding Revocation Messages over IPv4 using UDP encapsulation. For example, the source UDP port number, the destination UDP port number, the source IPv4 address, and the destination IPv4 address of the Binding Revocation Indication message are set to the destination UDP port number, the source UDP port number, destination IPv4 address, and source IPv4 address of the latest received and successfully processed Proxy Binding Update or Binding Update message, respectively. For more details on tunneling Proxy Mobile IPv6 and Mobile IPv6 signaling messages over IPv4, see [RFC5844] and [RFC5555], respectively.

5. Binding Revocation Message

This section defines the Binding Revocation Message format using an MH Type 16 as illustrated in Figure 4. The value in the Binding Revocation Type field defines whether the Binding Revocation Message is a Binding Revocation Indication or Binding Revocation Acknowledgement. If the Binding Revocation Type field is set to 1, the Binding Revocation Message is a Binding Revocation Indication as in Section 5.1. However, if the value is 2, it is a Binding Revocation Acknowledgement message as in Section 5.2.

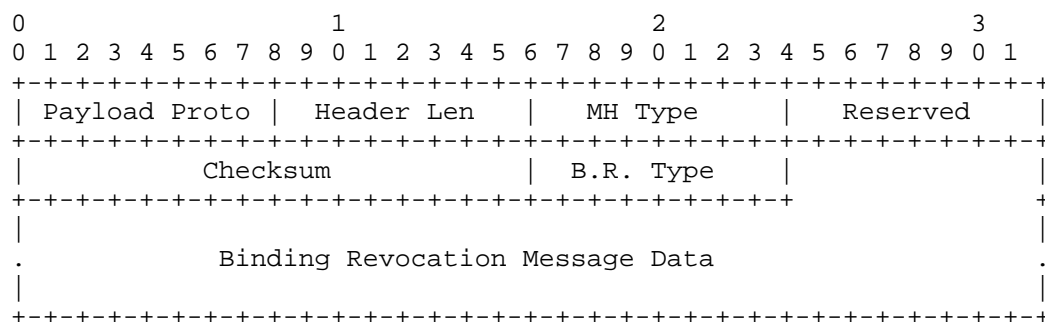


Figure 4: Binding Revocation Message

Payload Proto

8-bit selector. See [RFC3775] for more details.

Header Len

8-bit unsigned integer. Representing the length of the Mobility Header in units of 8 octets, excluding the first 8 octets. See [RFC3775] for more details.

MH Type

16, which identifies the mobility message as a Binding Revocation Message.

Reserved

8-bit field reserved for future use. The value MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Checksum

16-bit unsigned integer. This field contains the checksum of the Mobility Header. The checksum is calculated as described in [RFC3775].

Binding Revocation Type

8-bit unsigned integer. It defines the type of the Binding Revocation Message. It can be assigned one of the following values:

- 0 Reserved
- 1 Binding Revocation Indication
- 2 Binding Revocation Acknowledgement

All other values are unassigned

Binding Revocation Message Data

The Binding Revocation Message Data follows the Binding Revocation Message format that is defined in this document for the specified value in the Binding Revocation Type field. In this document, it is either a Binding Revocation Indication as in Section 5.1 or Binding Revocation Acknowledgement as in Section 5.2.

5.1. Binding Revocation Indication Message

The Binding Revocation Indication (BRI) message is a Binding Revocation Message that has an MH type 16 and a Binding Revocation Type value of 1. It is used by the initiator to inform the responder of the identity of a specific binding or bindings for which IP mobility service are being revoked. Binding Revocation Indication message is sent as described in Sections 7, 8.1, and 9.2.

When the value 1 is indicated in the Binding Revocation Type field of the Binding Revocation Message, the format of the Binding Revocation Message Data follows the Binding Revocation Indication message as in Figure 5

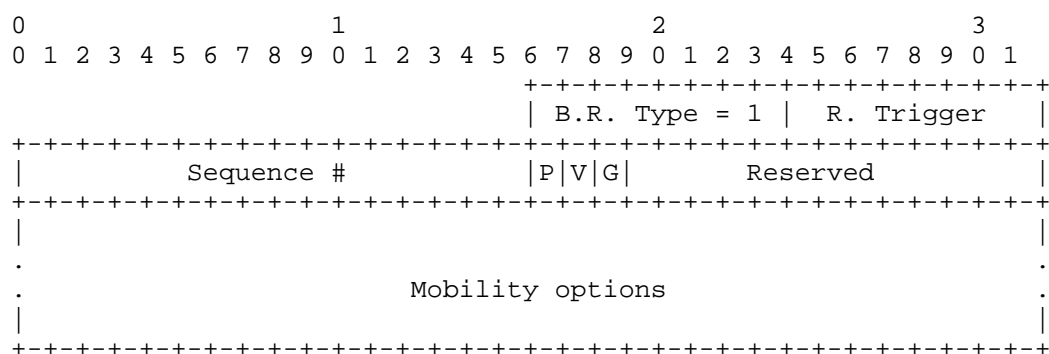


Figure 5: Binding Revocation Indication Message

Revocation Trigger

8-bit unsigned integer indicating the event that triggered the initiator to send the BRI message. The Per-MN Revocation Trigger values are less than 128. The Per-MN Revocation Trigger is used when the BRI message intends to revoke one or more bindings for the same mobile node. The Global Revocation Trigger values are greater than 128 and less than 250 and used in the BRI message when the Global (G) bit is set for global revocation. The values 250-255 are reserved for testing purposes only. The following Revocation Trigger values are currently defined:

Per-MN Revocation Trigger Values:

- 0 Unspecified
- 1 Administrative Reason
- 2 Inter-MAG Handover - same Access Type
- 3 Inter-MAG Handover - different Access Type
- 4 Inter-MAG Handover - Unknown
- 5 User-Initiated Session(s) Termination

- 6 Access Network Session(s) Termination
- 7 Possible Out-of-Sync BCE State

Global Revocation Trigger Values:

- 128 Per-Peer Policy
- 129 Revoking Mobility Node Local Policy

Reserved Revocation Trigger Values:

- 250-255 Reserved For Testing Purposes only
- All other values are Reserved

Sequence Number

A 16-bit unsigned integer used by the initiator to match a returned Binding Revocation Acknowledgement with this Binding Revocation Indication. This sequence number could be a random number. At any time, implementations MUST ensure there is no collision between the sequence numbers of all outstanding Binding Revocation Indication Messages.

Proxy Binding (P)

The Proxy Binding (P) bit is set by the initiator to indicate that the revoked binding(s) is a PMIPv6 binding.

IPv4 HoA Binding Only (V)

The IPv4 HoA Binding Only (V) bit is set by the initiator, home agent, or local mobility anchor to indicate to the receiving mobility entity the termination of the IPv4 Home Address binding only as in Sections 7 and 8.1.

Global (G)

The Global (G) bit is set by the initiator, LMA or MAG, to indicate the termination of all Per-Peer mobility Bindings or Multiple Bindings that share a common identifier(s) and are served by the initiator and responder as in Sections 8.1 and 9.2.

Reserved

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

Mobility Options

A 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 that it does not understand. These mobility options are used by the responder to identify the specific binding or bindings that the initiator is requesting be revoked.

The following options are valid in a Binding Revocation Indication:

- o Home Network Prefix option [RFC5213]. This option MAY be used only when the (P) bit is set. This option MUST be present when the BRI is used to revoke a single Proxy MIPv6 Binding Cache entry.
- o Mobile Node Identifier option [RFC4283]. This option MUST be present when the (P) bit is set. Additionally, if the Global (G) bit is set by the mobile access gateway, this option MUST carry the MAG identity. In this specification, only the Mobile Node Identifier option with subtype 1 is required and other subtypes are currently not supported.
- o Binding Identifier mobility option [RFC5648]. This option MUST be present if the initiator requests to terminate one binding of a multiple care-of address bindings for the same mobile node. The initiator may include more than one of the BID mobility options.
- o IPv4 Home Address option, which contains the mobile node home IPv4 address [RFC5555]. This option MUST only be included when the IPv4 HoA Binding only (V) bit is set and the (P) bit is cleared.
- o IPv4 Home Address Request option, which contains the mobile node proxy home IPv4 address [RFC5844]. This option MUST only be included when the IPv4 HoA Binding only (V) and the (P) bits are set.
- o Alternate Care-of Address mobility option [RFC3775]. According to [RFC5213], the mobile access gateway is allowed to include this option in the Proxy Binding Update to indicate the proxy care-of address of the mobile node mobility session. This option MAY be included to indicate the proxy care-of address of the mobile node's binding that is being revoked. In the case when the Global (G) bit is set, this option identifies all mobility bindings that share the same proxy care-of address.

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

5.2. Binding Revocation Acknowledgement Message

The Binding Revocation Acknowledgement (BRA) message is a Binding Revocation Message that has an MH type 16 and a Binding Revocation Type value of 2. It is used to acknowledge the receipt of a Binding Revocation Indication message described in Section 5.1. This packet is sent as described in Section 6.1.2.

When the value 2 is indicated in the Binding Revocation Type field of the Binding Revocation Message, the format of the Binding Revocation Message Data follows the Binding Revocation Acknowledgement message as in Figure 6.

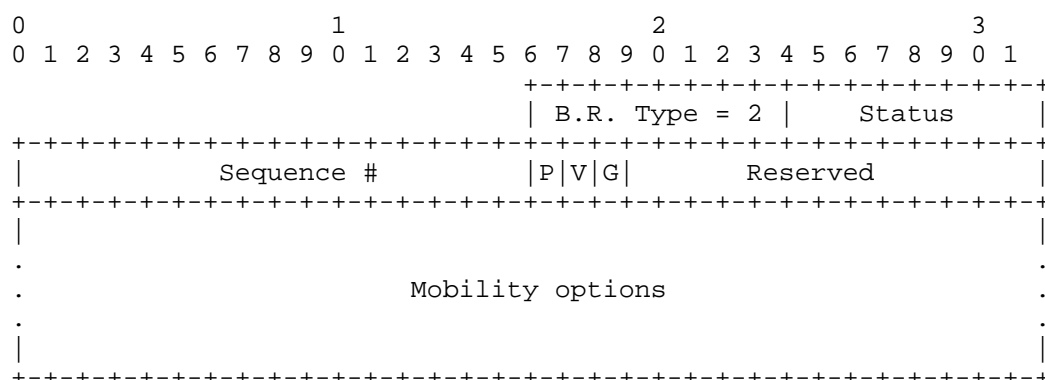


Figure 6: Binding Revocation Acknowledgement Message

Status 8-bit unsigned integer indicating the result of processing the Binding Revocation Indication message by the responder. Values of the Status field less than 128 indicate that the Binding Revocation Indication was processed successfully by the responder. Values greater than or equal to 128 indicate that the Binding Revocation Indication was rejected by the responder. The following Status values are currently defined:

- 0 success
- 1 partial success
- 128 Binding Does NOT Exist
- 129 IPv4 Home Address Option Required
- 130 Global Revocation NOT Authorized
- 131 Revoked Mobile Nodes Identity Required
- 132 Revocation Failed - MN is Attached
- 133 Revocation Trigger NOT Supported
- 134 Revocation Function NOT Supported
- 135 Proxy Binding Revocation NOT Supported

Sequence Number

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 initiator, e.g., HA, LMA, MAG, in matching this Binding Revocation Acknowledgement with the outstanding Binding Revocation Indication.

Proxy Binding (P)

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

IPv4 HoA Binding Only (V)

The IPv4 HoA Binding Only (V) bit is set if the (V) 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 Binding Revocation Indication message.

Reserved

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

Mobility Options

A 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 mobility options are valid in a Binding Revocation Acknowledgement:

- o Home Network Prefix option [RFC5213]. This option MAY be included only when the (P) bit is set.
- o Mobile Node Identifier Option [RFC4283]. This option MAY be included when the (P) bit is set. This option SHOULD be included if the Home Network Prefix option is included.

- o Binding Identifier mobility option [RFC5648]. The responder MAY include this option to indicate the specific BID that failed the revocation procedure.

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

6. Binding Revocation Process Operation

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

6.1. Sending Binding Revocation Message

When sending a Binding Revocation message, the initiator constructs the packet as it would do with any other Mobility Header with the exception of setting the MH Type field to 16.

The Binding Revocation Message MUST be protected using the same underlying security association, e.g., IPsec, that is being used between the two peers to protect the mobile node's Mobile IPv6 and its extensions binding registration signaling. If IPsec is not used as the underlying security mechanism to protect the binding registration signaling, the used underlying security mechanism MUST provide protection against all identified security threats as described under "Security Considerations" in [RFC3775] and [RFC5213].

6.1.1. Sending Binding Revocation Indication

The initiator MUST construct the Binding Revocation Message Data following the format of the Binding Revocation Indication message as described in Section 5.1 and the following:

- o The initiator MUST set the Sequence Number field to a valid sequence number for Binding Revocation. Since sending a Binding Revocation Indication message 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 associated Binding Revocation Indication using the Sequence Number field only.
- o If the initiator is revoking a binding that was created using proxy MIPv6 registration, the initiator MUST set the Proxy Binding (P) bit.

- o If the initiator is sending the Binding Revocation Indication message to revoke multiple mobility sessions, the initiator MUST set the Global (G) bit. In this case, the initiator MUST set the Revocation Trigger field to a valid value from the list of Global Revocation Triggers.
- o If the initiator is sending the Binding Revocation Indication message with the Global (G) bit cleared, the initiator MUST set the Revocation Trigger field to a valid value from the list of Per-MN Revocation Triggers.
- o If the initiator is sending the Binding Revocation Indication message to indicate the revocation of the mobile node IPv4 HoA Binding Only, the initiator MUST set the (V) bit. In this case, the initiator MUST include either the IPv4 Home Address option or the IPv4 Home Address Request option in the BRI to identify the IPv4 HoA that is being revoked.

6.1.2. Sending Binding Revocation Acknowledgement

The responder MUST send a Binding Revocation Acknowledgement message to indicate the receipt and the status of processing of the corresponding Binding Revocation Indication message as follows:

- o Whenever the Binding Revocation Indication is discarded, e.g., as described in Section 6.2, a Binding Revocation Acknowledgement MUST NOT be sent. Otherwise, the treatment depends on the following rules.
- o If the responder accepts the Binding Revocation Indication message, the responder MUST send a successful Binding Revocation Acknowledgement with an appropriate status code.
- o If the responder rejects the Binding Revocation Indication message, the responder MUST send a Binding Revocation Acknowledgement with an appropriate failure status code.

If the Source Address field of the IPv6 header that carried the Binding Revocation Indication message does not contain a unicast address, the Binding Revocation Indication packet MUST be silently discarded.

When the responder acknowledges the received Binding Revocation Indication message, the responder MUST construct the Binding Revocation Message Data following the format of the Binding Revocation Acknowledgement message as described in Section 5.2 and the following:

- o The responder MUST set the Sequence Number field by copying the value from the Sequence Number field of the received Binding Revocation Indication.
- o The responder MUST set the Status field to a valid value that reflects the status of the processing of the received Binding Revocation Indication message.
- o If the (P) bit is set in the received Binding Revocation Indication, the responder MUST set the (P) bit in the Binding Revocation Acknowledgement.
- o If the Global (G) bit is set in the received Binding Revocation Indication, the responder MUST set the Global (G) bit in the Binding Revocation Acknowledgement.
- o If the IPv4 HoA Binding Only (V) bit is set in the received Binding Revocation Indication, the responder MUST set the (V) bit in the Binding Revocation Acknowledgement.
- o 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.

6.2. Receiving Binding Revocation Message

When receiving a Binding Revocation Message, the responder MUST verify the Mobility Header as described in Section 9.2. of [RFC3775]. If the packet is dropped due to failing any of the Mobility Header test checks, the responder MUST follow the processing rules as in Section 9.2 of [RFC3775]. If the responder does not support the Binding Revocation Indication message and does not recognize the MH type 16, it sends a Binding Error message with the Status field set to 2 as described in [RFC3775].

Upon receiving a packet carrying a Binding Revocation Message, BRI or BRA, the receiving mobility entity MUST verify that the packet was received protected by the security association that is being used to protect the binding registration and Binding Revocation signaling between the two peers, e.g., an IPsec Security Association (SA).

6.2.1. Receiving Binding Revocation Indication

When the responder receives a packet carrying a Binding Revocation Indication message that was successfully processed as in Section 6.2, the responder, in addition, processes the message as follows:

- o The responder MUST validate that the Binding Revocation Indication is formatted as in Section 5.1.
- o If the Revocation Trigger field is set to a value that the responder does not support, the responder SHOULD reject the Binding Revocation Indication message using status code "Revocation Trigger NOT Supported".
- o If the Revocation Trigger value is NOT allowed with the Binding Revocation Indication message intent, e.g., the Global (G) bit is set and the Revocation Trigger field value is Per-MN-specific, the responder SHOULD reject the Binding Revocation Indication message using status code "Revocation Function NOT Supported".
- o If the responder failed to identify the mobile node(s) bindings as identified in the Binding Revocation Indication message, the responder MUST reject the BRI using status code "Binding Does NOT Exist".

6.2.2. Receiving Binding Revocation Acknowledgement

When the initiator receives a packet carrying a Binding Revocation Acknowledgement message that was successfully processed as in Section 6.2, the initiator, in addition, processes the message and examines the Status field as follows:

- o The initiator MUST validate that the sequence number in the 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 a sequence number of any of the outstanding Binding Revocation Indication messages, the initiator MUST silently discard the message but MAY log the event.
- o If the Status field indicates that the Binding Revocation Indication was processed successfully, the initiator MUST delete the current timer and the mobile node(s) binding(s) and all associated resources.
- o If the Status field indicates any value other than success, the initiator SHOULD examine any mobility options included in the Binding Revocation Acknowledgement. In this case, it is based on the initiator local policy how to handle the mobile node binding. The initiator MAY log the appropriate event to reflect the received status.

6.3. Retransmission of Binding Revocation Indication

If the initiator does not receive a Binding Revocation Acknowledgement in response to the outstanding Binding Revocation Indication before the InitMINDelayBRIs timer expires, the initiator, e.g., LMA, SHOULD retransmit the same BRI message up to the BRIMaxRetriesNumber as defined in Section 11.

The retransmissions by the initiator MUST use an exponential back-off process in which the timeout period is doubled upon each retransmission, until either the initiator receives a response or the timeout period reaches the value MAX_BRACK_TIMEOUT. The initiator MAY continue to send these messages at this slower rate up to the BRIMaxRetriesNumber.

If the initiator does not receive a Binding Revocation Acknowledgement message after the BRIMaxRetriesNumber of retransmits have been sent, the initiator SHOULD clean up all resources associated with this mobile node binding. The initiator may log the event.

7. Home Agent Operation

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:

- o The Revocation Trigger field MUST be set 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.
- o The Binding Revocation Indication MUST be sent using a Type 2 routing header that contains the mobile node's registered IPv6 home address for the binding being revoked.
- o The care-of address for the binding MUST be used as the destination address in the packet's IPv6 header.
- o If the home agent needs to only revoke the mobile node's IPv4 home address binding, the home agent MUST set the IPv4 HoA Binding Only (V) bit and MUST include the mobile node's registered IPv4 home address that is being revoked in the IPv4 Home Address option.

When the home agent sends 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

InitMINDelayBRIs timer. The home agent maintains the mobile node BCE in this state until it receives a Binding Revocation Acknowledgement or retransmits the Binding Revocation Indication message as described in Section 6.3.

In a race condition case, the home agent may receive a Binding Update from the mobile node while the mobile node's BCE has the revocation in progress flag set, the home agent SHOULD handle this case based on the reason for sending the Binding Revocation Indication message and its local policy. In this case, if the home agent accepts the Binding Update, it needs to update the mobile node BCE accordingly, e.g., removing the revocation in progress flag.

When the home agent needs to revoke one or more of a mobile node bindings that were created using multiple care-of address registrations as in [RFC5648], the home agent MUST include all the related BID mobility options that identify these bindings in the Binding Revocation Indication message. In the case when the home agent needs to revoke all of the mobile node bindings, the home agent SHOULD NOT include any of the BID mobility options.

When the home agent receives a packet carrying a valid Binding Revocation Acknowledgement message, the home agent follows Section 6.2 in processing this message.

8. Local Mobility Anchor Operation

8.1. Sending Binding Revocation Indication

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

- o The Proxy Binding (P) bit MUST be set to indicate that the binding being revoked is a PMIPv6 binding.
- o The Revocation Trigger field MUST be set to indicate to the mobile access gateway the reason for removing the specified mobile node PMIPv6 binding at the local mobility anchor. The Revocation Trigger may be used by the mobile access gateway to learn the mobile node's latest movement.
- o The packet MUST contain the Mobile Node Identifier (MN-ID) option, which contains the mobile node's Network Access Identifier (NAI) that was used in the Proxy Binding Update during the mobile node registration.

- o If the Mobile Node Identifier (MN-ID) is registered in more than one of the mobile node's BCEs and the local mobility anchor does NOT need to revoke all of the mobile node's bindings, the Binding Revocation Indication message MUST contain another identifier to uniquely identify the mobile node binding(s) that is being revoked, e.g., at least one Home Network Prefix option that contains the mobile node's registered Home Network Prefix (HNP) for the binding being revoked.
- o In the case of revoking all Per-Peer bindings, the local mobility anchor MUST set the Global (G) bit and the Revocation Trigger MUST contain the value "Per-Peer Policy" to request the mobile access gateway to remove all Per-Peer bindings that are registered with the local mobility anchor and this mobile access gateway.
- o The proxy care-of address for the binding MUST be used as the destination address in the packet's IPv6 header. However, in the case when IPsec is used to protect the Proxy MIPv6 signaling as specified in [RFC5213], the destination address MUST be set to the mag_address that is being used for keying the IPsec SA. If the mag_address is different than the mobile node proxy care-of address, the Alternate Care-of Address option MUST be included and MUST contain the mobile node proxy care-of address.

The local mobility anchor MAY delete the mobile node(s) IP tunnel immediately after sending the initial Binding Revocation Indication and before receiving the Binding Revocation Acknowledgement message.

When the local mobility anchor sends 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 InitMINDelayBRIs 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 that indicates inter-MAG handover, the local mobility anchor MAY switch the mobile node IP tunnel to the target mobile access gateway before sending the Binding Revocation Indication to the source mobile access gateway.

In a race condition case, the local mobility anchor may receive a Proxy Binding Update from the mobile access gateway while the mobile node's proxy BCE has the revocation in progress flag set. The local mobility anchor should handle this case based on the reason for sending the Binding Revocation Indication message and its local

policy. In this case, if the local mobility anchor accepts the Proxy Binding Update, it needs to update the mobile node proxy BCE accordingly, e.g., removing the revocation in progress flag.

When the local mobility anchor needs to revoke all the mobile node proxy BCEs that are registered with the local mobility anchor and the mobile access gateway peer, it MUST set the Global (G) bit and set 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 this Binding Revocation Indication message.

When the local mobility anchor needs to revoke all mobile nodes proxy BCEs that belong to a specific realm and are registered with the local mobility anchor and the mobile access gateway peer, the local mobility anchor MUST set the Global (G) bit and set the value of the Revocation Trigger field to "Revoking Mobility Node Local Policy". In this case, the local mobility anchor MUST include a mobility option in the Binding Revocation Indication that is shared among all the impacted mobile nodes BCEs, e.g., the mobile node identifier option, MN-ID option, with a subtype value of 1. In this case, the NAI value in the MN-ID MUST follow the format where the content after the "@" character defines the realm that is shared amongst all of the impacted mobile nodes proxy BCEs. As an example: @example.com identifies all mobile nodes whose MN-ID value contains "example.com" as the realm, e.g., "1234abdelta@example.com", "axxyzd@example.com", and "abcdefg.xyz123@example.com", but not "1234abdelta@foo.example.com".

When the local mobility anchor needs to revoke a subgroup of the mobile nodes proxy BCEs that belong to a specific realm and are registered with the local mobility anchor and the mobile access gateway, the local mobility anchor MUST set the Global (G) bit and set the value of the Revocation Trigger field to "Revoking Mobility Node Local Policy". In this case, the local mobility anchor MUST include an additional mobility option to the mobile node identifier option (MN-ID) option, with a subtype value of 1. In other words, the impacted mobile node BCEs are those that have an MN-ID with a realm as specified above and, e.g., are assigned the same proxy care-of address as the one included in the Alternate Care-of Address mobility option.

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

According to the Proxy Mobile IPv6 specification [RFC5213], if the local mobility anchor receives a Proxy Binding Update message from a new mobile access gateway for extending the binding lifetime of the only BCE of this mobile node with the Handoff Indicator value set to "Handoff state unknown (4)", the local mobility anchor waits a period of MaxDelayBeforeNewBCEAssign to receive a de-registration message from the previous mobile access gateway before updating the mobile node's BCE with the new point of attachment. If a de-registration message is not received, the local mobility anchor considers the received Proxy Binding Update message as a request for a new BCE and if processed successfully, the local mobility anchor assigns a different HNP for the new BCE.

This document updates the local mobility anchor's behavior in this case. If the local mobility anchor supports the binding revocation mechanism as described in this document, it SHOULD proactively send a Binding Revocation Indication message to the previous mobile access gateway instead of waiting for a de-registration from the previous mobile access gateway. In the Binding Revocation Indication message, the Revocation Trigger MUST be set to "Inter-MAG Handover - Unknown".

If the local mobility anchor sent a Binding Revocation Indication message with the Revocation Trigger field set to "Inter-MAG Handover - Unknown" and while waiting for a response, Binding Revocation Acknowledgement, the following are possible conditions that the local mobility anchor MUST handle as specified below:

- o If the local mobility anchor receives a successful Binding Revocation Acknowledgement message or a de-registration message from the previous mobile access gateway, the local mobility anchor MUST update the mobile node BCE as if it received a de-registration message as described in [RFC5213].
- o If the local mobility anchor receives a Binding Revocation Acknowledgement message with the Status field set to "Revocation Failed - MN is Attached", the local mobility anchor SHOULD update the mobile node BCE as if it did NOT receive a de-registration before the MaxDelayBeforeNewBCEAssign timer expired by creating a new BCE as described in [RFC5213].
- o If the local mobility anchor did not receive a Binding Revocation Acknowledgement message or a de-registration Proxy Binding Update from the previous mobile access gateway after it exhausted all of the Binding Revocation Indication message retransmissions as described in Section 6.3, the local mobility anchor SHOULD update the mobile node's BCE as if it did NOT receive a de-registration before the MaxDelayBeforeNewBCEAssign timer expired by creating a new BCE as described in [RFC5213]. Note that the local mobility

anchor SHOULD use the recommended number of retransmissions for the Binding Revocation Indication message as described in Section 11 to avoid delaying the creation of a new Binding Cache entry for too long, if the mobile node is actually attaching to the new MAG with a different interface.

When the mobile node is registered with an IPv4 proxy home address in addition to the Home Network Prefix where both of the IPv4 proxy HoA (pHoA) and HNP are bound to the same proxy CoA (pCoA), the local mobility anchor MAY revoke the mobile node IPv4 proxy HoA binding to the current mobile node proxy CoA while maintaining the mobile node binding of the HNP to its current pCoA as part of the mobile node BCE. In this case, if the local mobility anchor decides to revoke the mobile node IPv4 proxy HoA only, it MUST send a Binding Revocation Indication message following the procedure in Section 6.1 and the following rules:

- o The IPv4 HoA Binding Only (V) bit MUST be set in the BRI to indicate that only the IPv4 home address binding is being revoked.
- o The IPv4 Home Address Request option MUST be included with the mobile node's registered proxy home IPv4 address that is being released in addition to the MN-ID option.
- o The mobile node Home Network Prefix option MUST NOT be included.
- o The Revocation Trigger field MUST be set to an appropriate value, e.g., "User Initiated Session(s) Termination".

8.2. 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 processes the message as follows:

- o If the (P) bit is set, the local mobility anchor MUST validate that all impacted bindings have the proxy binding flag set.
- o If the Global (G) bit is set and the Revocation Trigger field value is "Per-Peer Policy", the LMA MUST validate that the Proxy (P) bit is set and the MN-ID option is present with the mobile access gateway identity included. In addition, 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 global revocation with revocation trigger value "Per-Peer Policy", see Section 13. If the local mobility anchor processes the Global

Binding Revocation Indication message successfully, it MUST accept the Binding Revocation Indication message using the status code "success".

- o If the mobile access gateway is not authorized to use the Per-Peer Global revocation feature or the received Binding Revocation Indication message has the Global (G) bit set and the Revocation Trigger field is set to "Per-Peer Policy", but the MN-ID option is not included, the local mobility anchor MUST reject the Binding Revocation Indication message using status code "Global Revocation NOT Authorized".
- o If the Global (G) bit is set and the Revocation Trigger value is "Per-Peer Policy", and only the mobile node identifier (MN-ID) option is included, the local mobility anchor MUST revoke all mobile node bindings for which the proxy CoA is the one used as the source of the IPv6 packet that carried the Binding Revocation Indication. However, if the Alternate Care-of Address option is included in addition to the mobile node identifier option, the local mobility anchor MUST revoke all mobile node bindings whose proxy care-of address matches the care-of address in the Alternate Care-of Address option. After the local mobility anchor successfully processes the Binding Revocation Indication message and identifies all impacted mobile nodes bindings, it MUST accept the Binding Revocation Indication message using the status code "success".
- o If the local mobility anchor accepted the Binding Revocation Indication message but one or more of the bindings identified in the received Binding Revocation Indication message has already been released, the local mobility anchor MUST accept the message and it MAY set the Status field to "partial success" and include the mobile node identifier (MN-ID) or the Home Network Prefix option to identify the binding(s) that failed the revocation procedure.
- o If the Global (G) bit is not set, the local mobility anchor uses 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 accept the message and revoke all bindings for this mobile node that use the specified mobile node NAI including the IPv4 Home Address binding(s) if present.

2. If the mobile node identifier (MN-ID) and one Home Network Prefix option are included, the local mobility anchor MUST accept the message and only remove the specified mobile node 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 MUST accept the message and remove all bindings that are referenced by these Home Network Prefixes for the specified mobile node NAI.
4. If the IPv4 HoA binding Only (V) bit is set and the mobile node identifier (MN-ID) option and the IPv4 Home Address Request option are included, the local mobility anchor MUST accept the message and remove only the IPv4 HoA address binding to the mobile node current proxy care-of address.

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 that track the state of the peer mobile access gateway.

After the local mobility anchor accepts or rejects a Binding Revocation Indication message, the local mobility anchor MUST follow Sections 6.1 and 6.1.2 to send a Binding Revocation Acknowledgement message to the mobile access gateway.

9. Mobile Access Gateway Operation

9.1. Receiving Binding Revocation Indication

When the mobile access gateway receives a packet carrying a Binding Revocation Indication that was successfully processed as in Section 6.2, the mobile access gateway processes the message as follows:

- o If the Global (G) bit is set and the Revocation Trigger field value is "Per-Peer Policy", the mobile access gateway MUST validate that the Proxy (P) bit is set and no mobility options are included in the message. If the mobile access gateway processes the Global Binding Revocation Indication message successfully, it MUST accept the Binding Revocation Indication message using the status code "success".
- o If the Global (G) bit is set and the Revocation Trigger field value is "Revoking Mobility Node Local Policy", the mobile access gateway MUST validate that the Proxy (P) bit is set and at least the MN-ID option with the subtype value of 1 is included in the

Binding Revocation Indication and it is formatted as described in Section 8.1. If the mobile access gateway processes this Global Binding Revocation Indication message successfully, it MUST accept the message using the status code "success".

- o If the Global (G) bit is set and the Revocation Trigger field value is "Revoking Mobility Node Local Policy", and no mobility options are included in the Binding Revocation Indication message or the mobile access gateway is not able to identify the impacted mobile nodes bindings based on the included mobility options, the mobile access gateway MUST treat this as an error scenario. In this case, the mobile access gateway MUST reject the Binding Revocation Indication message using status code "Revoked Mobile Nodes Identity Required".
- o If the Revocation Trigger field value in the received Binding Revocation Indication message indicates inter-MAG handover, e.g., Inter-MAG Handover - Unknown, the mobile access gateway uses the mobility option(s) included in the Binding Revocation Indication message to identify the mobile node binding. The mobile access gateway SHOULD ensure that the mobile node is no longer attached to the mobile access gateway before accepting the BRI message using status code "success". However, if the mobile access gateway verified that the mobile node is still directly attached, the mobile access gateway MUST reject the BRI using status code "Revocation failed - MN is Attached".
- o If the IPv4 HoA Binding Only (V) bit is set, the mobile access gateway uses the MN-ID option to identify the mobile node binding entry in the Binding Update List (BUL). The mobile access gateway MUST verify that the IPv4 address included in the IPv4 Home Address Request option in the received Binding Revocation Indication is the same as the IPv4 proxy HoA that is assigned to the mobile node. After the mobile access gateway successfully validates the received IPv4 home address as the mobile node IPv4 HoA, it MUST consider this as an indication to ONLY release the mobile node IPv4 proxy HoA binding to the mobile node current proxy CoA. Consequently, it MUST continue to maintain the mobile node IPv6 proxy HoA or HNP binding to the current mobile node proxy CoA as part of the mobile node binding in the BUL entry and release all resources associated with the MN IPv4 proxy HoA binding to the MN pCoA. If the mobile access gateway processed the BRI successfully, the mobile access gateway MUST accept the BRI using status code "success". On the other hand, if the mobile access gateway is able to identify the mobile node binding using the MN-ID but failed to identify the received IPv4 proxy HoA, the mobile access gateway MUST reject the BRI using status code "Binding Does NOT Exist".

- o If the mobile access gateway accepts the Binding Revocation Indication message but one or more of the bindings identified in the received Binding Revocation Indication message has already been released before processing the Binding Revocation Indication, the mobile access gateway MUST accept the Binding Revocation Indication message. In this case, the mobile access gateway MAY set the Status field to "partial success" and 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 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 HNP has been terminated, e.g., if the Revocation Trigger field is set to "Administrative Reason", the mobile access gateway may terminate the IPv6 or IPv4 mobility session on the access link and notify the mobile node. The specific details and considerations on how the mobile access gateway terminates IPv6 or IPv4 mobility session on the access link and notifies the mobile node can be found in [RFC5213] and [RFC5844].

After the mobile access gateway accepts or rejects a Binding Revocation Indication message, the mobile access gateway MUST follow Sections 6.1 and 6.1.2 to send a Binding Revocation Acknowledgement message to the local mobility anchor.

9.2. Sending Binding Revocation Indication

The mobile access gateway could send a Binding Revocation Indication message to indicate the termination of multiple mobile node bindings, e.g., when using the global revocation with the Global (G) bit set. In this case, when an event occurs that requires the mobile access gateway to inform the local mobility anchor peer to terminate all mobile node bindings that are registered at the local mobility anchor and the mobile access gateway, the mobile access gateway sends a Binding Revocation Indication message following the procedure in Section 6.1 and the following:

- o The Proxy Binding (P) bit MUST be set to indicate that the binding(s) being revoked is a PMIPv6 binding.
- o 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 the mobile access gateway. In this case, the MN-ID option MUST be included in the Binding Revocation Indication and contain

the mobile access gateway identity. In addition, the mobile access gateway MAY include the Alternate Care-of Address option. If included, the Alternate Care-of Address option MUST contain the proxy care-of address the bindings that are being impacted by this Binding Revocation Indication message.

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

As described in Section 6.3, the mobile access gateway SHOULD retransmit the 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 node IP tunnels immediately after sending the Binding Revocation Indication and before receiving a Binding Revocation Acknowledgement message from the LMA.

In response to a Binding Revocation Indication message, if the mobile access gateway receives a packet carrying a Binding Revocation Acknowledgement that was successfully processed as in Section 6.2 and 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 set and the Revocation Trigger field value set to "Per-Peer Policy" 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

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:

- o The mobile node MUST verify that the IP address in the Type 2 routing header is its Home Address and that its Binding Update List contains an entry for that Home Address. If one of the tests fails, the mobile node SHOULD silently discard the received Binding Revocation Indication message.
- o If mobile node Binding Update List contains an entry for the IP address in the Type 2 routing header of the received Binding Revocation Indication packet, the mobile node MUST accept the BRI message using status code "success".
- o If the IPv4 HoA Binding Only (V) bit is set in the received BRI message, the mobile node MUST verify that there is an IPv4 Home Address option in the received Binding Revocation Indication and

the IPv4 address included in the IPv4 Home Address option is the same as its IPv4 HoA that is assigned to the mobile node. If this verification is successful, the mobile node MUST consider this Binding Revocation Indication as an indication to ONLY release the mobile node IPv4 HoA binding to its current care-of address. Consequently, the mobile node MUST continue to maintain its IPv6 HoA binding to the current CoA as part of the mobile node binding in the BUL entry and release all resources associated with the MN IPv4 HoA binding. In this case, the mobile node MUST accept the Binding Revocation Indication message using status code "success". On the other hand, if the IPv4 Home Address Option was NOT included in the received BRI with the (V) bit is set, the MN MUST reject the BRI message with status code "IPv4 Home Address Option Required". Additionally, if the IPv4 HoA received in the IPv4 Home Address Option is NOT the one assigned to the mobile node, the mobile node SHOULD reject the Binding Revocation Indication with status code "Binding Does NOT Exist".

- o 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 reject the Binding Revocation Indication using status code "Proxy Binding Revocation NOT Supported".
- o 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 Binding Revocation Indication message. If the mobile node received a Binding Revocation Indication with one or more BID options and its home address is included in the Type 2 routing header, the mobile node MUST consider all of the care-of addresses bindings, identified in the BID options, with this home address as being revoked. In this case, if the BRI validation is successful, the mobile node MUST accept the Binding Revocation Indication message with status code "success".
- o If the mobile node has multiple care-of address bindings with its home agent and received a Binding Revocation Indication, without any BID option included and its home address was included in the Type 2 routing header, the mobile node MUST consider all of its registered care-of address bindings with this home address as being revoked. If the mobile node validates the BRI successfully, the mobile node MUST accept the Binding Revocation Indication message with status code "success".

If the mobile node accepts or rejects the Binding Revocation Indication message, the mobile node MUST follow Sections 6.1 and 6.1.2 to send a Binding Revocation Acknowledgement message to the home agent. Note that anytime the MN does not send a Binding

Revocation Acknowledgement to a BRI, the initiator is likely to retransmit the BRI at least one time. This causes additional load on the initiator who sends the retransmissions, as well as on the MN that will receive and process them.

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.

11. Protocol Configuration Variables

Any mobility entity that 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.

Initial Minimum Delay Between BRI messages (InitMINDelayBRIs)

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

Maximum BRA TIMEOUT (MAX_BRACK_TIMEOUT)

This variable specifies the maximum delay timeout in seconds before the revoking mobility entity retransmits a BRI message. The default is 2 seconds.

12. IANA Considerations

This specification defines a new Binding Revocation Message using a new Mobility Header Type 16, as described in Section 5. The new Mobility Header type value needs to be assigned from the same numbering space as allocated for the other Mobility Header types registry.

This document also creates a new registry "Binding Revocation Type" that indicates the type of the binding revocation message. The current binding revocation message types are described in Sections 5.1 and 5.2, and are the following:

- 0 Reserved
- 1 Binding Revocation Indication
- 2 Binding Revocation Acknowledgement
- All other values are unassigned

Future values of the Binding Revocation Type can be allocated using Standards Action or IESG Approval [RFC5226].

In addition, this document also creates a second new registry for the Revocation Trigger that indicates the reason behind sending the Binding Revocation Indication message. The current Revocation Trigger values are described in Section 5.1, and are the following:

Per-MN Revocation Trigger Values:

- 0 Unspecified
- 1 Administrative Reason
- 2 Inter-MAG Handover - same Access Type
- 3 Inter-MAG Handover - different Access Type
- 4 Inter-MAG Handover - Unknown
- 5 User-Initiated Session(s) Termination
- 6 Access Network Session(s) Termination
- 7 Possible Out-of-Sync BCE State

Global Revocation Trigger Values:

- 128 Per-Peer Policy
- 129 Revoking Mobility Node Local Policy

Reserved Revocation Trigger Values:

- 250-255 Reserved For Testing Purposes only
- All other values are Unassigned

Future values of the Revocation Trigger can be allocated using Standards Action or IESG Approval [RFC5226].

Furthermore, this document creates a third new registry "Binding Revocation Acknowledgement Status Codes". The current values are described in Section 5.2, and are the following:

- 0 success
- 1 partial success
- 128 Binding Does NOT Exist
- 129 IPv4 Home Address Option Required
- 130 Global Revocation NOT Authorized
- 131 Revoked Mobile Nodes Identity Required
- 132 Revocation Failed - MN is Attached
- 133 Revocation Trigger NOT Supported
- 134 Revocation Function NOT Supported
- 135 Proxy Binding Revocation NOT Supported

Future values of the Status field can be allocated using Standards Action or IESG Approval [RFC5226].

All fields labeled "Reserved" are only to be assigned through Standards Action or IESG Approval.

13. Security Considerations

This specification allows the mobility node that initiates the binding revocation procedure to revoke a mobility session(s) that is currently registered with it. It is NOT allowed for any mobility node to revoke a mobile node mobility session that is not registered with this mobility node.

The binding revocation protocol described in this specification uses the same security association between the mobile node and the home agent or the mobile access gateway and the local mobility anchor that is being used to exchange the MIPv6 or PMIPv6 Binding Update and Binding Acknowledgement signaling. If IPsec is used, the traffic selectors associated with the Security Policy Database (SPD) entry protecting the Binding Update and Binding Acknowledgement MUST be extended to include Binding Revocation Message MH type 16. Extending the traffic selectors of the SPD entry in order to reuse the SA protecting the Binding Update and Binding Acknowledgement (instead of creating new ones) ensures that those SAs will be up and running when the revoking entity needs to send a binding revocation signaling message.

On the other hand, if IPsec is not used as the underlying security mechanism to protect the Mobile IPv6 and its extensions binding registration signaling, the used underlying security mechanism MUST provide protection against all identified security threats as described under "Security Considerations" in [RFC3775] and [RFC5213].

Since some mobility entities, e.g., local mobility anchor and mobile access gateway, are allowed to send and receive Binding Revocation Indications and Binding Revocation Acknowledgements for different cases, when IPsec is used to secure signaling between the local mobility anchor and mobile access gateway, it prevents any of them from processing a Binding Revocation Message that was not constructed by an authorized party.

The Proxy Mobile IPv6 [RFC5213] requires the local mobility anchor to restrict the creation and manipulation of proxy bindings to specifically authorized mobile access gateways. Therefore, the mobile access gateway that is authorized to create or manipulate the mobile node proxy BCE is also authorized to revoke such mobile node registration by sending a de-registration with lifetime of zero.

However, since bulk termination using Binding Revocation Indication with the Global (G) bit set and the Revocation Trigger field set to "Per-Peer Policy" impacts all mobility sessions that are registered with the mobile access gateway and its local mobility anchor peer, the local mobility anchor MUST be locally configurable to authorize such specific functionality. Additional mechanisms, such as a policy store or Authentication, Authorization, and Accounting (AAA) may be employed, but these are outside the scope of this specification.

14. Acknowledgements

The authors would like to thank Ryuji Wakikawa, Bruno Mongazon-Cazavet, Domagoj Premec, Arnaud Ebalard, Patrick Stupar, Vijay Devarapalli, and Joel Hortelius for their review and comments of this document and all colleagues who have supported the advancement of this effort.

Also, we would like to thank Jari Arkko, Ben Campbell, Pasi Eronen, Ralph Droms, Alexey Melnikov, Tim Polk, Adrian Farrel, and Robert Sparks for their reviews of this document as part of the IESG review process.

15. References

15.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
- [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.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

- [RFC5648] Wakikawa, R., Devarapalli, V., Tsirtsis, G., Ernst, T., and K. Nagami, "Multiple Care-of Addresses Registration", RFC 5648, October 2009.
- [RFC5555] Soliman, H., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

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
Ericsson, Inc.
2201 Lakeside Blvd.
Richardson, TX 75082
USA

EMail: ahmad.muhanna@ericsson.com

Mohamed Khalil
Ericsson, Inc.
6300 Legacy Dr.
Plano, TX 75024
USA

EMail: mohamed.khalil@ericsson.com

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

EMail: sgundave@cisco.com

Kuntal Chowdhury
Cisco
30 International Place
Tewksbury, MA 01876
USA

EMail: kchowdhu@cisco.com

Parviz Yegani
Juniper Networks
1194 North Mathilda Avenue
Sunnyvale, CA 94089
USA

EMail: pyegani@juniper.net

