

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 15, 2008

A. Lindem
A. Oswal
Redback Networks
February 12, 2008

Bulk Registration Revocation in Mobile IPv4
draft-acee-mip4-bulk-revocation-01.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/lid-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 August 15, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Internet-Draft

Mobile IPv4 Bulk Revocation

February 2008

Abstract

This document describes an extension to Mobile IPv4 Registration Revocation (as described in [RFC 3543](#)) for a home or foreign agent to revoke mobile IP services for multiple bindings or visitors with a single registration revocation exchange.

Table of Contents

1.	Introduction	3
1.1.	Requirements notation	3
2.	Registration Revocation Extensions and Messages	4
2.1.	Revocation Support Extension Changes	4
2.2.	Revocation Selection Extension	5
2.3.	Registration Revocation Message Changes	8
2.4.	Registration Revocation Acknowledgment Message Changes . .	10
2.5.	Replay Protection	11
2.6.	GRE Key Applicability	11
3.	Bulk Registration Revocation Overview	12
3.1.	Home Agent Responsibilities	12
3.2.	Foreign Agent Responsibilities	12
3.3.	Direct Co-located Node Responsibilities	13
4.	Security Considerations	14
5.	IANA Considerations	15
6.	References	16
6.1.	Normative References	16
6.2.	Informative References	16
Appendix A.	Acknowledgments	17
Appendix B.	Change Log	18
B.1.	Changes from 00 Version to 01 Version	18
	Authors' Addresses	19
	Intellectual Property and Copyright Statements	20

[1.](#) Introduction

This document describes an extension to Mobile IPv4 Registration Revocation (as described in [[REVOCATION](#)]) for a home or foreign agent to revoke mobile IP services for multiple bindings or visitors with a single registration revocation exchange.

[1.1.](#) Requirements notation

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

[2.](#) Registration Revocation Extensions and Messages

The following changes are required for bulk revocation.

1. The revocation support extension will include a bit indicating whether or not the agent supports bulk revocation.
2. The Registration Revocation and Registration Revocation Acknowledgment will include a bit indicating whether or not the registration is a bulk registration. If so, the Home Agent Address will include a prefix rather than a specific mobile node's home address. Additionally, a previously reserved field will now include the prefix length.
3. A non-skippable revocation selection extension is added to further qualify bulk Registration Revocation.

[2.1.](#) Revocation Support Extension Changes

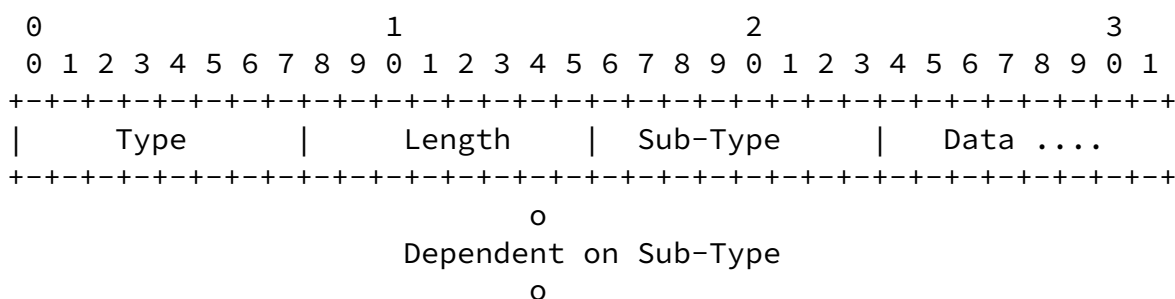
The Mobile IP Revocation Support Extension indicates support of registration revocation, and so MUST be attached to a Registration Request or Registration Reply by any entity that wants to receive revocation messages. The extension is fully described in [\[REVOCATION\]](#). This document includes an indication of whether or not bulk revocation is supported for this registration. Alternately, bulk revocation could be negotiated globally between the mobility agents using a mechanism beyond the scope of this specification.

revocation support will only be in force when negotiated by both agents through either the setting of the 'B' bit or a global mechanism beyond the scope of this specification.

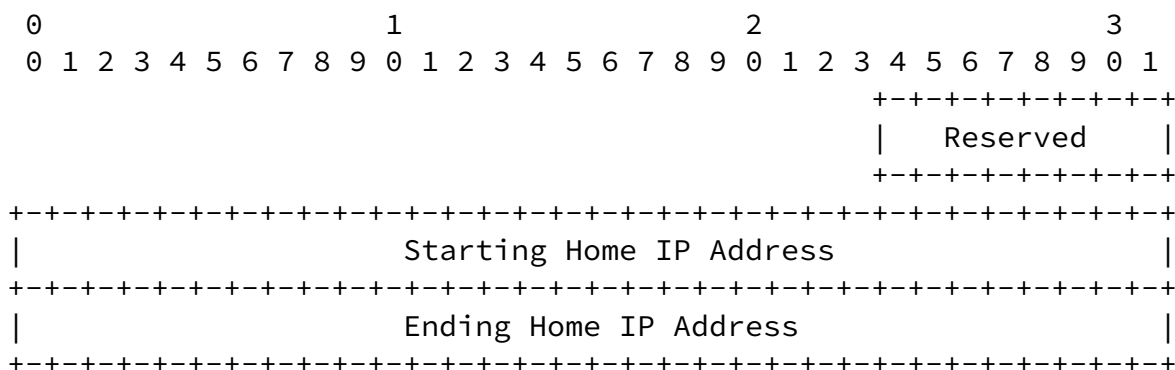
2.2. Revocation Selection Extension

The Mobile IP Revocation Selection Extension is used to further qualify bulk revocation (as described herein). It is only applicable to the Registration Revocation and Registration Revocation Acknowledgement messages.

The format of the Revocation Selection Extension is based on the Type-Length-Sub-Type-Value Short Extension Format described in [MIP4]. It further qualifies the selection of revoked registrations specified herein.



Revocation Selection Extension



Start/End Home IP Address Sub-Type Variable Format

1 - Start/End Home IP Address

Indicates the TLV contains a starting and ending home IP address used to further qualify registration selection. For this sub-type, the length of the TLV will be 10 bytes.

2 - NAI Regular Expression

Indicates the TLV contains a regular expression applied to the NAI (Network Access Identifier). This field is only limited by the single byte length. Hence, it can be up to 254 octets in length given that the sub-type takes 1 octet.

3 - Encapsulation

Indicates the TLV contains a tunnel encapsulation protocol identifier. This indicates that the bulk revocation only applies to registrations using the specified tunnel encapsulation. For this sub-type, the length of the TLV will be 2 bytes.

Reserved

Reserved for future use. MUST be set to 0 on sending, MUST be ignored on receiving.

Starting Home IP Address

The starting address in a range of IP home addresses whose registrations are to be revoked.

Ending Home IP Address

The ending address in a range of IP home addresses whose registrations are to be revoked.

NAI Regular Expression

A regular expression to be matched against the Network Address Identifier (NAI) for registration to determine which registrations are to be revoked. Refer to [\[NAI\]](#) for information on Mobile IP Network Access Identifiers. Refer to [\[REG-EXPR\]](#) for information on regular expressions.

The protocol ID corresponding to the tunnel encapsulation:

- 94 IP-in-IP encapsulation [[IP-IN-IP](#)]
- 47 Generic Routing Encapsulation (GRE) [[GRE](#)]
- 55 Minimal IP Encapsulation [[MIN-IP](#)]

The Mobile IP revocation selection extension may appear in either a Registration Revocation or Registration Revocation Acknowledgement message.

[2.3.](#) Registration Revocation Message Changes

The Registration Revocation Message is fully described in [[REVOCATION](#)]. The UDP header is followed by the Mobile IP fields which are repeated herein with the changes described below:

0										1										2										3															
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1														
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Type										Reserved										A		I		B		Reserved										Prefix Len									
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Home Address/Prefix																																													
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Home Domain Address																																													
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Foreign Domain Address																																													
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Revocation Identifier																																													
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Extensions...																																													
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														
Authenticator...																																													
+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+														

Registration Revocation Message Changes

Changes to the Registration Revocation message are:

Type

7 - Unchanged from [[REVOCATION](#)]

'I' Bit

Unchanged from [[REVOCATION](#)]

'A' Bit

Unchanged from [[REVOCATION](#)]

'B' Bit

This bit is set to '1' by a mobility agent to indicate that this revocation message is a request for bulk revocation. Bulk revocation may apply to one or many registrations.

Reserved

Reserved for future use. MUST be set to 0 on sending, MUST be ignored on receiving.

Prefix Length

The prefix length which, when combined with the home prefix specifies which registrations are to be revoked. If bulk revocation is requested (as specified by the 'B' bit) and this field is zero, the Registration Revocation applies to all registrations for which bulk revocation was previously negotiated using the Revocation Support Extension or a global mechanism beyond the scope of this specification.

Reserved

Reserved for future use. MUST be set to 0 on sending, MUST be ignored on receiving.

Home Address/Prefix

If bulk revocation is requested ('B' bit set to '1'), this field is combined with the prefix length to select one or more registrations to be revoked. If bulk revocation is not requested ('B' bit set to '0'), this field specifies the home IP address of the mobile node whose registration is being revoked.

Home Domain Address

Unchanged from [[REVOCATION](#)]

Foreign Domain Address

Unchanged from [[REVOCATION](#)]

Revocation ID

Unchanged from [[REVOCATION](#)]

The Registration Revocation message is processed as before only now

it can be applied to one or more active registrations between the mobility agents. It must be authenticated as specified in [\[REVOCATION\]](#).

[2.4.](#) Registration Revocation Acknowledgment Message Changes

The Registration Revocation Acknowledgment Message is fully described in [\[REVOCATION\]](#). The UDP header is followed by the Mobile IP fields which are repeated herein with the changes described below:

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Type										Reserved										I B Reserved										Prefix Length									
Home Address																																							
Revocation Identifier																																							
Extensions...																																							
Authenticator...																																							

Registration Revocation Message Changes

Changes to the Registration Revocation Acknowledgement message are:

Type

15 - Unchanged from [\[REVOCATION\]](#)

'I' Bit

Unchanged from [\[REVOCATION\]](#)

'B' Bit

This bit is set to '1' by a mobility agent to indicate successful revocation of at least one registration in response to the bulk

revocation request.

Reserved

Reserved for future use. MUST be set to 0 on sending, MUST be ignored on receiving.

Prefix Length

The prefix length which, when combined with the home prefix specifies which registrations were revoked. The prefix length MUST match the length specified on the corresponding Registration Revocation message.

Reserved

Reserved for future use. MUST be set to 0 on sending, MUST be ignored on receiving.

Home Address/Prefix

If bulk revocation is requested ('B' bit set to '1'), this field is combined with the prefix length to select one or more registrations to be revoked. If bulk revocation is not requested ('B' bit set to '0'), this field specifies the home IP address of the mobile node whose registration is being revoked. It MUST match the home address/prefix specified on the previous Registration Revocation message.

Revocation ID

Unchanged from [[REVOCATION](#)]

A Registration Revocation Acknowledgment message MUST be sent in response to a valid and authenticated registration revocation message as specified in [[REVOCATION](#)].

[2.5.](#) Replay Protection

Replay protection proceeds in much the same way as described in [[REVOCATION](#)]. However, when assuring that the message is not a replayed message, the mobility agent must check the timestamp to assure it is greater than the timestamp received from the most

recently received Mobility Revocation Support extension from the agent. One way to support this is to maintain the most recent per-peer timestamp for peer mobility agents. For co-located mobile nodes, there normally will be only one active registration (situations where there are many are beyond the scope of this document).

[2.6.](#) GRE Key Applicability

If GRE keys are being utilized as described in [[MIP-GRE-KEY](#)], then the GRE Key Extension as described in the same document MUST be included in bulk registration revocation messages. If a Home Agent and Foreign Agent are using GRE tunnels with keys and a registration revocation is exchanged without the GRE Key Extension, it should be dropped by the recipient and the event should be logged.

[3.](#) Bulk Registration Revocation Overview

Bulk Registration Revocation processing is identical to Registration Revocation as described in [[REVOCATION](#)] except for following differences:

1. When the Registration Request is received, bulk revocation support is negotiated through the setting of the B-Bit in the Revocation Support extension. This negotiation should not preclude global bulk revocation negotiation between mobility agents. However, such support is beyond the scope of this document.
2. When a mobility agent processes a bulk Registration Revocation, it may apply to multiple registrations.
3. The replay protection validation will now use the timestamp in the most recent Revocation Support Extension from the sending agent. This is described in [Section 2.5](#).

[3.1.](#) Home Agent Responsibilities

Home Agent responsibilities are identical to [[REVOCATION](#)] except as noted above. In situations where a single event may apply to

multiple registrations (or bindings on the Home Agent), a bulk revocation may be sent in lieu of multiple revocations. A non-exhaustive list of events that may benefit from bulk revocation includes:

1. Graceful shutdown of the home agent (HA) instance
2. Policy changes that preclude communication with the Foreign Agent (FA)
3. Withdrawn of the Home Agent local address from service
4. Home Address Pool deletion or change
5. Other policy change resulting in multiple registrations being revoked

[3.2.](#) Foreign Agent Responsibilities

Foreign Agent responsibilities are identical to [\[REVOCATION\]](#) except as noted above. In situations where a single event may apply to multiple registrations (or visitors on the Foreign Agent), a bulk

revocation may be sent in lieu of multiple revocations. A non-exhaustive list of events that may benefit from bulk revocation includes:

1. Graceful shutdown of the foreign agent (FA) instance
2. Policy changes that preclude communication with the Home Agent (HA)
3. Withdrawn of the Care-of-Address (CoA) from service
4. Other policy change resulting in multiple registrations being revoked

[3.3.](#) Direct Co-located Node Responsibilities

In general, bulk revocation is not the useful to a direct co-located

node since it will usually only have single registration with a home agent. Hence, there is really no reason for a direct co-located to negotiate bulk revocation in the first place by setting the B-Bit in the Revocation Support Extension appending to its initial registration. However, this specification does not preclude support and a direct co-located node negotiating bulk revocation must support bulk revocation requests.

[4.](#) Security Considerations

Security is basically unchanged from [\[REVOCATION\]](#) with the exception that replay protection will be based on the most recent registration revocation received from the peer (as described in [Section 2.5](#)). As with [\[REVOCATION\]](#), all message exchanges related to revocation MUST be protected by either a valid authenticator as specified in [\[MIP4\]](#). For communications between mobility agents, FA-HA authentication or a mechanism at least as secure, e.g. IPsec, is required. For communication between a home agent and a direct co-located mobile node, MN-HA authentication or a mechanism at least as secure is

required. In this context, all message exchanges relating to revocation include Registration Revocations, Registration Revocation Acknowledgments, Registration Requests including the Revocation Support Extension, and Registration Replies including the Revocation Support Extension.

[5.](#) IANA Considerations

A non-skippable extension value is needed for the Revocation Selection Extension. This should be allocated from the "Extensions

appearing in Mobile IP messages" number space in the "Mobile IPv4 Numbers". Also, a new sub-registry is required for the sub-types for this extension. Initially, it will have the following values:

1 - Start/End Home IP Address

Indicates the TLV contains a starting and ending home IP address used to further qualify registration selection.

2 - NAI Regular Expression

Indicates the TLV contains a regular expression applied to the NAI (Network Access Identifier).

3 - Encapsulation

Indicates the TLV contains a tunnel encapsulation protocol identifier.

Refer to [Section 2.2](#) for more information.

[6.](#) References

[6.1.](#) Normative References

- [GRE] Farinacci, D., Li, T., Meyer, D., and P. Traina, "Generic Routing Encapsulation", [RFC 2784](#), March 2000.
- [IP-IN-IP] Perkins, C., "IP Encapsulation within IP", [RFC 2003](#), October 1996.
- [MIN-IP] Perkins, C., "Minimal Encapsulation within IP", [RFC 2004](#), October 1996.
- [MIP4] Perkins, C., "IP Mobility Support for IPv4", [RFC 3344](#), August 2002.
- [NAI] Johansson, F. and T. Johansson, "Mobile IPv4 Extension for Carrying Network Access Identifiers", [RFC 3846](#), June 2004.
- [REG-EXPR] Institute of Electrical and Electronix Engineers, "Information Technology - Portable Operation System Interface (POSIX) - Part 2: Shell and Variables (Vol. 1)", IEEE 1003.3, 1992.
- [REVOCATION] Chandra, M. and S. Glass, "Registration Revocation in Mobile IPv4", [RFC 3543](#), August 2003.
- [RFC-KEYWORDS] Bradner, S., "Key words for use in RFC's to Indicate Requirement Levels", [RFC 2119](#), March 1997.

[6.2.](#) Informative References

- [MIP-GRE-KEY] Yegani, P., Dommety, G., Lior, A., Chowdhury, K., and J. Navali, "GRE Key Extension for Mobile IPv4", [draft-yegani-gre-key-extension-03.txt](#) (work in progress).

[Appendix A](#). Acknowledgments

The RFC text was produced using Marshall Rose's xml2rfc tool.

Thanks to Hendrik Levkowetz and Sri Gundavelli for their comments on the document.

[Appendix B](#). Change Log

[B.1](#). Changes from 00 Version to 01 Version

The section contains list of changes from version 00 to version 01:

- o Change the prefix length field in the registration revocation message from 8 bits to 6 bits. Refer to [Section 2.3](#).
- o Add reference to GRE key draft and a section documenting the applicability to this document. Refer to [Section 2.6](#).

Authors' Addresses

Acee Lindem
Redback Networks
102 Carric Bend Court
Cary, NC 27519
USA

Email: acee@redback.com

Anand Oswal
Redback Networks
300 Holger
San Jose, CA 95134
USA

Email: aoswal@redback.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).