Network Working Group
Request for Comments: 3543
Category: Standards Track

S. Glass
Sun Microsystems
M. Chandra
Cisco Systems

August 2003

Registration Revocation in Mobile IPv4

Status of this Memo

Copyright Notice

Abstract

This document defines a Mobile IPv4 Registration Revocation mechanism whereby a mobility agent involved in providing Mobile IP services to a mobile node can notify the other mobility agent providing Mobile IP services to the same mobile node of the termination of this registration. The mechanism is also usable by a home agent to notify a co-located mobile node of the termination of its binding as well. Moreover, the mechanism provides for this notification to be acknowledged. A signaling mechanism already defined by the Mobile IPv4 protocol is leveraged as a way to inform a mobile node of the revocation of its binding.

Table of Contents

1. Introduction and Applicability

Mobile IP [1] defines registration of a mobile node's location to provide connectivity between the mobile node and its home domain, facilitating communication between mobile nodes and any correspondent node. At any time, either the home or foreign agent may wish to cease servicing a mobile node, or for administrative reasons may no longer be required to service a mobile node.

This document defines a general registration revocation mechanism for Mobile IPv4, whereby a mobility agent can notify another mobility agent (or a 'direct' co-located mobile node) of the termination of mobility bindings. A mobility agent that receives a revocation notification no longer has to provide services to the mobile node whose registration has been revoked. A signaling mechanism already defined by the Mobile IPv4 protocol [1] is leveraged as a way to inform a mobile node of the revocation of its binding.

The registration revocation protocol provides the following advantages:

1. Timely release of Mobile IP resources. Resources being consumed to provide Mobile IP services for a mobile node that has stopped receiving Mobile IP services by one agent, can be reclaimed by the other agent in a more timely fashion than if it had to wait for the binding to expire. This also applies to the case in which a mobile node roams away from a foreign agent to another foreign agent. Notification to the previous foreign agent would allow it to reclaim resources.

2. Accurate accounting. This has a favorable impact on resolving accounting issues with respect to the length of mobility bindings in both domains, as the actual end of the registration is relayed.

3. Earlier adoption of domain policy changes with regards to services offered/required of a Mobile IP binding. For example, the home domain may now require reverse tunnels [C], yet there are existing bindings that do not use them. Without a revocation mechanism, new services can only be put in place or removed as bindings are re-registered.

4. Timely notification to a mobile node that it is no longer receiving mobility services, thereby significantly shortening any 'black-hole' periods to facilitate a more robust recovery.

The revocation protocol is an active, yet unobtrusive mechanism allowing more timely communication between the three Mobile IP entities in the various administrative domains. Since many mobile nodes may not understand the concept of revocation, care has been taken to ensure backwards compatibility with [1].

The registration revocation protocol does not replace the methods described in [1] for Mobile IP deregistration, as the purpose of these mechanisms is fundamentally different. Deregistration messages are used by a mobile node to inform its home agent that it has e.g., roamed back to its home subnet, whereas revocation messages are used between mobility agents to signal the termination of mobility bindings. More specifically, the revocation message defined here is NOT for use by 'direct' co-located mobile nodes that are terminating their registration as deregistration messages are already sufficient for this purpose. A 'direct' co-located mobile node, however, may wish to process revocation messages as it is a useful mechanism to trigger the re-negotiation of required services from the home domain.

2. Terminology

It is assumed that the reader is familiar with the terminology used in [1]. In addition, the following terms are defined:

'Direct' Co-located Mobile Node

A mobile node registering directly with its home agent, with the 'D' bit set in its registration request, and NOT registering through a foreign agent.

Mobile IP Resources

Various functional elements allocated by a mobility agent to support a Mobile IP binding, e.g., memory.

Mobile IP Services

Various responsibilities of a mobility agent in supporting a mobile node as defined in [1], e.g., encapsulation of packets addressed to a mobile node by a home agent, decapsulation of these packets by a foreign agent for delivery to a mobile node, etc.

Mobility Agent

The home agent or foreign agent as specified in [1].

Revocation

Premature termination of a mobility binding.

The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [3].

3. Registration Revocation Extensions and Messages

Registration revocation in Mobile IPv4 is accomplished via the following:

- Advertising Registration Revocation Support (Section 3.1.):

  - o A flag in the Agent Advertisement extension has been reserved for agents to advertise their support of revocation messages.

- Revocation Support Extension (Section 3.2.):

  o This extension is appended to a registration request or registration reply by a mobility agent to indicate its support of registration revocation.

  o This extension is appended to a registration request by a 'direct' co-located mobile node to indicate its understanding of revocation messages.

- Registration Revocation Message (Section 3.3.):

  o A message sent by a mobility agent to inform another mobility agent, or a 'direct' co-located mobile node, that it has revoked the binding of a mobile node.

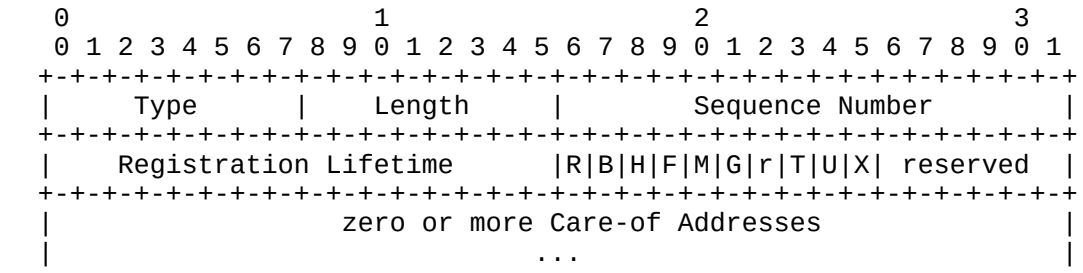
- Registration Revocation Acknowledgment Message (Section 3.4.):

  o A message sent by mobility agents or 'direct' co-located mobile nodes to indicate the receipt of a revocation message.

Security considerations related to the above messages and extensions are covered in Section 6.

3.1. Advertising Registration Revocation Support

Mobility agents can advertise their support of registration revocation with a modification to the Mobility Agent Advertisement extension described in [1]. An 'X' bit is introduced to indicate an agent's support for Registration Revocation.



X The mobility agent supports Registration Revocation

A foreign agent that sets the 'X' bit in an agent advertisement extension MUST support registration revocation messages on that link, specifically the Revocation Support Extension (section 3.2.), Revocation Messages (section 3.3.), and Revocation Acknowledgment

(section 3.4.). It is not required that all agents advertising on the same link support registration revocation, nor is it required that an agent advertise this support on all of its links.

Note that using this information, a mobile node can select a foreign agent that supports Registration Revocation. Should a mobile node not understand this bit, it simply ignores it as per [1].

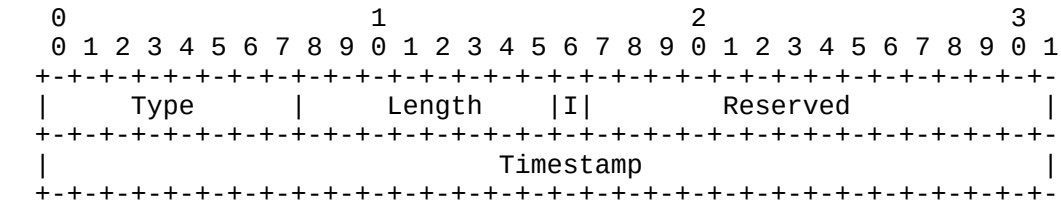
As a bit in the agent advertisement, use of the 'X' bit has no impact on other messages, such as e.g., Challenge-Response [2].

3.2. Revocation Support Extension

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. Normally, this is either a foreign agent, or a home agent. However a 'direct' co-located mobile node MAY also include a revocation support extension in its registration request. A mobile node which is not co-located MUST NOT include a Revocation Support Extension in its registration.

A foreign agent advertising the 'X' bit on the link on which the registration request was received, and that has a security relationship with the home agent identified in the same registration request, MUST attach a revocation support extension to the forwarded registration request. A home agent that receives a registration request that does not contain a revocation extension SHOULD NOT include a revocation support extension in the associated registration reply.

The format of the revocation support extension is based on the Type-Length-Value Extension Format given in [1] and is defined as follows:



Type 137

Length

Length (in bytes, currently 6). Does NOT include Type and Length fields (in accordance with section 1.9. of [1]). This allows for a longer extension length should more bits be required in the future.

Timestamp

Current 4-byte timestamp of the mobility agent or 'direct' co-located mobile node. This is used to identify the ordering of registrations as they are forwarded, how they relate to the sending of any revocation messages, and to identify the approximate offset between the clocks of the mobility agents providing support for this binding, or between a 'direct' co-located mobile node and its home agent.

'I' Bit

This bit is set to '1' by a mobility agent to indicate it supports the use of the 'I' bit in revocation messages (section 3.3.)

When sent by a foreign agent in a registration request:

If set to 1, the FA is willing to have the home agent use the 'I' bit in the revocation process to determine whether the mobile node should be informed of the revocation or not.

If set to 0, indicates to the home agent that the foreign agent will follow its own policy with regards to informing the mobile node in the event of a revocation.

When sent by a home agent in response to a revocation extension in which the 'I' bit was set to '1':

If set to 1, the home agent agrees to use the 'I' bit in the revocation process to indicate to the foreign agent whether or not the mobile node should be informed.

If set to 0, the home agent will not use the 'I' bit in the revocation process, thereby yielding to the foreign agent's default behavior with regard to informing the mobile node.

To preserve the robustness of the protocol, the recommended default behavior for a foreign agent is to inform the mobile node of its revocation as described in Section 4.1.

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

When appearing in a registration request, or registration reply, the Mobile IP revocation support extension MUST be protected either by a foreign-home authentication extension, a mobile-home authentication extension, or any other equivalent mechanism [1], e.g., via AAA [A], [B], or perhaps IPsec. If the extension appearing in either of these registration messages is NOT protected, the appropriate action as described by [1] (Sections 3.8.2.1. and Sections 3.7.3.1.) MUST be taken.

Support of the 'I' bit is OPTIONAL. If a mobility agent does not support the specified functionality, it MUST set the 'I' bit to zero. Note that the home agent setting the 'I' bit to '1' in response to a revocation extension from the foreign agent in which the 'I' bit was set to '0' is undefined, and SHOULD NOT be done.

'I' bit support has been negotiated when both agents have set the 'I' bit to '1' in their revocation support extensions.

It is important to note that this extension is skippable (i.e., if the receiving mobility agent does not understand this extension, it MUST skip it, and continue processing the remainder of the registration request).

3.3. Registration Revocation Messages

A revocation message is sent by a mobility agent to inform another mobility agent, or a 'direct' co-located mobile node, that it is revoking the binding of a mobile node.

IP Fields:

Source Address
: In the case of the home agent issuing the registration revocation, the address registered with the care-of address as that of the home agent (that is the address identified as the home address of this binding).

  In the case of the foreign agent issuing the registration revocation, the address registered with the home agent as the care-of address.

Destination Address In the case of the home agent issuing the registration revocation, the source address of the last approved registration request for this binding, i.e., the destination address of the last registration reply indicating success for this binding.

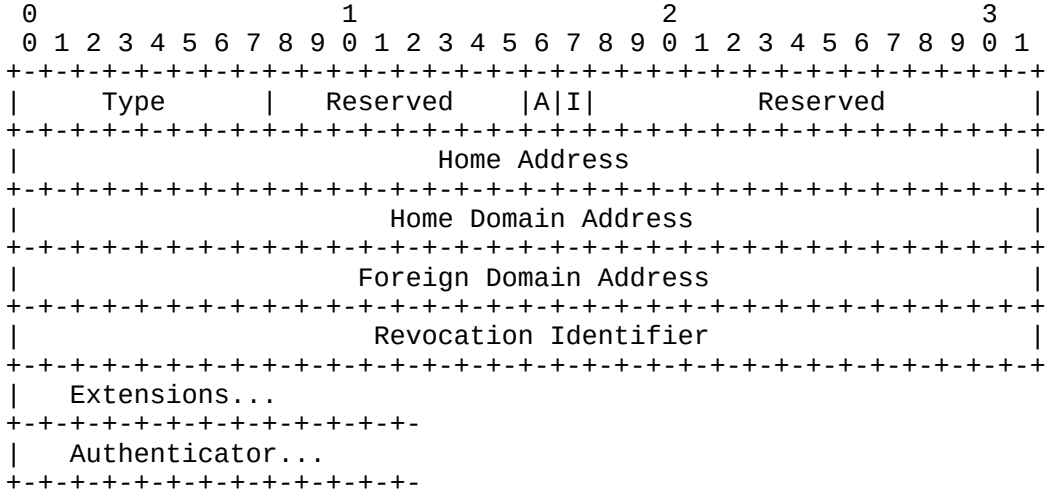
In the case of the foreign agent issuing the registration revocation, the address registered as that of the home agent by the mobile node whose registration is being revoked.

UDP Fields:

Source Port variable

Destination Port 434

The UDP header is followed by the Mobile IP fields shown below:



Type 7

Reserved MUST be sent as 0, ignored when received.

A Agent bit ('direction' bit).

This bit identifies the role of the agent sending the revocation, that is the 'direction' of the revocation message. This is useful for detecting reflection

attacks, particularly when symmetric keying is being used.

Set to '0' if the revoking agent is servicing this binding as a foreign agent.

Set to '1' if the revoking agent is servicing this binding as a home agent.

I Inform bit.

This bit MUST NOT be set to '1' unless 'I' bit support was negotiated in the revocation extension messages passed in the registration process, otherwise the results can be unpredictable.

When sent by the home agent to a foreign agent:

Set to '0' to request that the mobile node SHOULD NOT be informed of the revocation, or because the use of the 'I' bit was not agreed upon.

Set to '1' to request that the mobile node be informed of the revocation.

When sending a revocation message to a 'direct' co-located mobile node, this bit is essentially irrelevant, but SHOULD be set to '1'.

When sent by the foreign agent:

Set to '0' to indicate that the foreign agent is using foreign domain policy as to whether or not the mobile node should be informed of the revocation, or because 'I' bit support was not agreed upon.

Set to '1' to ask the home agent if the mobile node should be informed of the revocation.

Reserved
MUST be sent as 0, ignored when received.

Home Address
The home IP address of the mobile node whose registration is being revoked.

Foreign Domain Address
: The relevant IP address in the foreign domain to identify which binding is being revoked. This is one of the following: (i) the foreign agent's IP address, or (ii) the co-located care-of address.

Home Domain Address
: The IP address of the home agent to identify which binding is being revoked.

Revocation Identifier
: Protects against replay attacks. The revoking agent MUST insert its current 4-byte timestamp running off the same clock as it is using to fill in the timestamp in its revocation extensions. See section 3.5.

A registration revocation message MUST be protected by either a valid authenticator as specified in [1], namely a home-foreign authenticator, if the communication is between home and foreign agents, or a mobile-home authenticator if the communication is being sent from a home agent to a 'direct' co-located mobile node, or another security mechanism at least as secure, and agreed upon by the home and foreign domains, e.g., IPsec. If any agent, or 'direct' co-located mobile node, receives a registration revocation message that does not contain a valid authenticator, and is not adequately protected, the revocation message MUST be ignored, and silently discarded.

A revocation message MUST NOT be sent for any registration that has expired, and MAY only be sent prior to the expiration of a mobile node's registration. Note, however, due to the nature of datagram delivery, this does not guarantee these messages will arrive before the natural expiration of any binding.

An agent MUST NOT send more than one revocation message or registration message per second for the same binding. Note that this updates [1] by including revocation messages in the rate limit specified in [1], i.e., that an agent MUST NOT send more than one registration message per second for the same binding.

An example of the use of revocation messages is given in Appendix A.

3.4. Registration Revocation Acknowledgment Message

A revocation acknowledgment message is sent by mobility agents or 'direct' co-located mobile nodes to indicate the successful receipt of a revocation message.

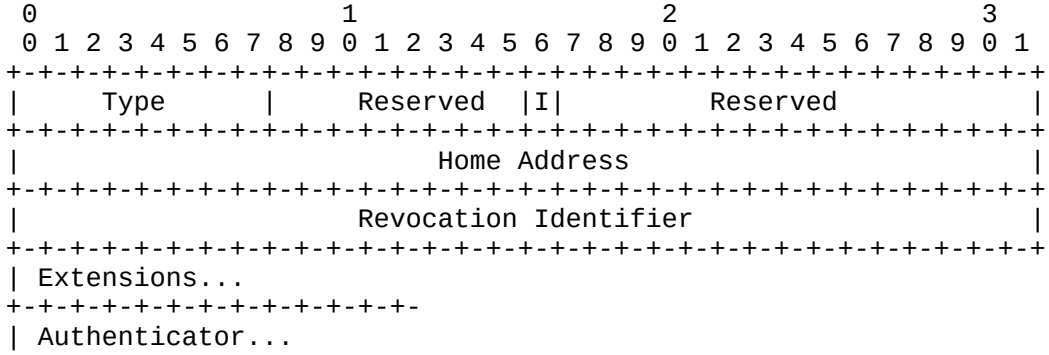
IP fields:

Source Address	Copied from the destination address of the received registration revocation message for which this registration revocation acknowledgment message is being generated.
Destination Address	Copied from the source address of the received registration revocation message for which this registration revocation acknowledgment message is being generated.

UDP fields:

Source Port	434 (copied from the destination port of the revocation message).
Destination Port	Copied from the source port of the revocation message.

The UDP header is followed by the Mobile IP fields shown below:



Type 15

Reserved
MUST be sent as 0, ignored when received.

I Inform bit.

The 'I' bit MUST NOT be set to '1' in the revocation acknowledgment messages unless it was set to '1' in the revocation message. If an agent receives a revocation acknowledgment message in which the 'I' bit is set to '1', but for which the revocation message being

acknowledged had the 'I' bit set to '0', the 'I' bit in the revocation acknowledgment message MUST be ignored.

When sent by the home agent:

Set to '1' by the home agent to request the foreign agent inform the mobile node of the revocation.

Set to '0' by the home agent to request the foreign agent not inform the mobile node of the revocation.

When sent by a foreign agent:

Set to '1' to indicate to the home agent that the mobile node was informed.

Set to '0' to indicate to the home agent that the foreign agent used local policy to determine whether or not the mobile node should be informed. For purposes of protocol robustness, it is highly recommended that such a default be set for the foreign agent to inform the mobile node of the revocation.

Reserved
: MUST be sent as 0, ignored when received.

Home Address
: The home address copied from the revocation message for which this acknowledgment is being sent.

Revocation Identifier
: Copied from the Revocation Identifier of the revocation message for which this acknowledgment is being sent. See Section 3.5.

A registration revocation acknowledgment message MUST be sent in response to a valid and authenticated registration revocation message.

A registration acknowledgment message MUST be protected by either a valid authenticator as specified in [1], namely a home-foreign authenticator if the communication is between home and foreign agents, or a mobile-home authenticator if the communication is between home agent and 'direct' co-located mobile node, or another security mechanism at least as secure and agreed upon by the home and foreign domains, e.g., IPsec.

An example of the use of Revocation Acknowledgment Messages is given in Appendix A.

3.5. Replay Protection

As registration revocation messages are designed to terminate service for a mobile node, or multiple mobile nodes simultaneously, replay protection is crucial to prevent denial of service attacks by "malicious repeaters" - those who store datagrams with the intent of replaying them at a later time, or by "malicious reflectors" - those who reflect packets back at their original source (both a form of "active" attack). See Section 6. for a discussion of these security considerations.

All Revocation Messages and Revocation Acknowledgment Messages MUST be authenticated as well be replay-protected. The order in which they are done, however, is up to implementation.

Replay protection is handled with a simple timestamp mechanism, using a single 32-bit identifier field in the registration revocation message, in conjunction with the home address field, to associate any revocation acknowledgment messages with its revocation messages. To do this:

- The revoking agent sets the 'A' bit to its agent-type, and the Revocation Identifier field in the registration revocation message to a valid 32-bit timestamp from the same clock it is using to set the timestamp field of its revocation extensions included in registration messages.

- Upon receipt of an authenticated revocation message, the receiving agent (or 'direct' co-located mobile node) MUST check the value of the 'A' bit, and Revocation Identifier to make sure this revocation message is not a replay of an old revocation message received from the same agent. The receiving agent MUST also check that the message is not a reflection of a revocation message it sent in relation to the identified binding. If the 'A' bit and Identifier field imply this packet is a replay, the revocation message MUST be silently discarded.

- When building a revocation acknowledgment message, the acknowledging agent (or 'direct' co-located mobile node) copies the values of the Home Address and Revocation Identifier fields from the revocation message into the Home Address and the Revocation Identifier of the revocation acknowledgment message. This is so the revoking agent can match this revocation acknowledgment to its corresponding revocation message.

- Upon receiving a valid revocation acknowledgment, the revoking agent MUST check the Home Address and Identifier fields to make sure they match those fields from a corresponding revocation message it sent to the acknowledging agent. If not, this revocation acknowledgment message MUST be silently discarded.

Note that since the Identifier in an incoming revocation message is a 32-bit timestamp, it is possible for an agent to check the validity of the Identifier fields without having to remember all identifiers sent by that corresponding agent.

Note: as it is possible for a mobile node to register at different times with different home agents, and at different times with different foreign agents, it is crucial that it not be required that the Identifier fields be unique in messages from different agents as there is no guarantee that clocks on different agents will be synchronized. For example, if a mobile node has simultaneous bindings with multiple foreign agents, and if revocation messages are received by more than one such foreign agent "simultaneously", it is possible the revocation message from one of these foreign agents may contain Identifier fields that happen to match those of any or all the other foreign agents. This MUST NOT result in any of these revocation messages being ignored.

4. Registration Revocation Overview

Registration Revocation consists of two distinct pieces: a signaling mechanism between tunnel endpoints, and a signaling mechanism between foreign agent and mobile node. A 'direct' co-located mobile node MAY implement revocation extensions and revocation acknowledgment in order to receive and respond to revocation messages from its home agent, however, a 'direct' co-located mobile node MUST NOT send a revocation message as de-registration messages defined in [1] are sufficient for this purpose.

For further discussion on security issues related to registration revocation, refer to Section 6.

4.1. Mobile Node Notification

A mechanism which provides a foreign agent a way to actively notify a mobile node that its binding has been reset already exists in [1], though it has been overlooked for this purpose.

A brief overview of the mechanics of the sequence number in agent advertisement from [1] is given so that the mechanism by which the foreign agent 'implies' to the mobile node that its binding is no longer active is clearly understood.

When a foreign agent begins sending agent advertisements, it starts with a sequence number of 0, and [monotonically] increments the sequence number with each subsequent agent advertisement. In order for a mobile node to be able to distinguish between a foreign agent that has simply exhausted the sequence number space from one which has been reset, when the agent increments the sequence number counter past its maximum value, it sets the sequence number to 256 instead of rolling to 0 [1]. In this way, a mobile node would have to miss, at that time, 256 advertisements in a row to mistake a reset as a roll-over. Moreover, the lifetimes contained within an agent advertisement should be set in such a way that when a mobile node believes it has missed 3 beacons, the entry for this foreign agent should time out, and if the mobile node is registered there, it should send an agent solicitation [1]. If, however, an agent is somehow reset, it will begin advertising with a sequence number of 0, and the mobile node can presume this foreign agent has lost its binding, and the mobile node SHOULD re-register to make sure it is still obtaining Mobile IP services through this foreign agent.

Leveraging this mechanism, a foreign agent may consciously notify all mobile nodes currently bound to it that it has "reset" all of their bindings, even if the agent itself has not been reset, by simply [re]setting the sequence number of the next agent advertisement to 0. Moreover, a foreign agent may inform all mobile nodes currently bound to it that they should re-register with a different foreign agent by simultaneously setting the 'B' bit in the advertisement to 1, indicating this foreign agent is busy and is not accepting new registrations [1]. In these situations, any mobile node in compliance with [1] will presume this foreign agent has lost its binding, and must re-register if they wish to re-establish Mobile IP functionality with their home subnet.

To indicate to any registered mobile node that its binding no longer exists, the foreign agent with which the mobile node is registered may unicast an agent advertisement with the sequence number set to 0 to the mobile node [1], [D]. Moreover, if such a foreign agent wishes to indicate to the mobile node that its binding has been revoked, and that the mobile node should not attempt to renew its registration with it, the foreign agent MAY also set the 'B' bit to 1 in these agent advertisements, indicating it is busy, and is not accepting new registrations [1]. All mobile nodes compliant with [1] will understand that this means the agent is busy, and MAY either immediately attempt to re-register with another agent in their foreign agent cache, or MAY solicit for additional agents. In the latter case, a foreign agent can optionally remember the mobile node's binding was revoked, and respond to the solicit in the same way, namely with the 'B' bit set to 1. It should be noted, though, that since the foreign agent is likely to not be setting the 'B' bit

to 1 in its broadcasted agent advertisements (sent to the entire link), the revoked mobile node, upon hearing this agent's multicast agent advertisement without the 'B' bit set, may attempt to [re]register with it. If this happens, depending on foreign domain policy, the foreign agent can simply deny the mobile node with an appropriate error code (e.g., "administratively prohibited"). At this time, a mobile node can use foreign agent fallback to attempt to register with a different foreign agent as described in [1].

Mobile nodes which understand the revocation mechanism described by this document may understand that a unicast agent advertisement with the sequence number reset to 0 could indicate a revocation, and may attempt to re-register with the same foreign agent, or register with a different foreign agent, or co-locate.

Agent Advertisements unicast to a mobile node MUST be sent as described in [1] in addition to any methods currently in use on the link to make them secure or authenticatable to protect from denial-of-service attacks.

4.2. Registration Revocation Mechanism - Agent Notification

A foreign agent that is currently supporting registration revocation on a link MUST set the 'X' bit in its Agent Advertisement Extensions being sent on that link. This allows mobile nodes requiring Registration Revocation services to register with those foreign agents advertising its support.

4.2.1. Negotiation of Revocation Support

During the registration process, if the foreign agent wishes to participate in revocation messages with the home domain, it MUST have an existing security association with the home agent identified in the registration request, and append a revocation support extension (defined in Section 3.2.) to it. If the corresponding registration reply from this home agent does not contain a revocation support extension, the foreign agent SHOULD assume the home agent does not understand registration revocation, or is unwilling to participate. If this is unacceptable to the foreign agent, it MAY deny the registration with e.g., "Administratively Prohibited". Note that in this case, where a security association exists, as specified in [1], both registration request and registration reply MUST still contain home-foreign authenticators.

If a home agent wishes to be able to exchange revocation messages with the foreign domain, it MUST have an existing security association with the foreign agent who relayed the registration request, and it MUST append a revocation support extension to the

registration reply. If the registration request from a foreign agent did not contain a revocation support extension, the home agent SHOULD assume the foreign agent does not understand registration revocation, or is unwilling to participate specifically for this binding. If this is unacceptable to the home agent, it MAY deny the registration with e.g., "Administratively Prohibited". The home agent MAY include a revocation support extension in the registration reply.

If a 'direct' co-located mobile node wishes to be informed of a released binding by its home agent, it MUST insert a revocation support extension into the registration request. If this is acceptable to the home agent, it MUST include a revocation support extension in its registration reply. Note that if this is not acceptable, the home agent MAY deny the registration, or it MAY simply not include a revocation support extension in its registration reply indicating to the mobile node that it will not participate in revocation for this binding. A home agent which receives a registration request from a 'direct' co-located mobile node which does not contain a revocation support extension MAY deny the registration with e.g., "Administratively Prohibited" and also MAY or MAY NOT include a revocation support extension in the registration reply.

Note that a non-colocated mobile node MUST NOT insert a revocation support extension into its registration request. If a foreign agent receives such a registration request, it MUST silently discard it, and MAY log it as a protocol error.

The 'I' bit in the revocation extension is used to indicate whether or not the decision to inform the mobile node that its binding is terminated will be left to the home agent. This functionality is offered by the foreign agent, and accepted by the home agent. More precisely, by sending a revocation extension attached to a registration request in which the 'I' bit is set to 1, the foreign agent is indicating to the home agent that it MAY leave the decision to inform this mobile node that its registration is terminated up to the home agent. (The term "MAY" is used here because it is recognized that domain policy may change during the lifetime of any registration). The home agent can acknowledge that it wishes to do this by setting the 'I' bit to 1, or it can indicate it will not do so by setting the 'I' bit to 0, in the revocation extension appearing in the registration reply.

Revocation support is considered to be negotiated for a binding when both sides have included a revocation support extension during a successful registration exchange.

4.2.2. Home Domain Revoking/Releasing a Registration

The following section details the responsibilities of each party depending on the functionality negotiated in the revocation support extensions when the home domain is revoking a registration.

4.2.2.1. Home Agent Responsibilities

In the case where a home agent is revoking a mobile node's binding, and revocation support has been negotiated, the home agent MUST notify the foreign domain address it is terminating the tunnel entry point by sending a revocation message. Note that the foreign domain address can either be the foreign agent care-of address, or the co-located care-of address of a 'direct' co-located mobile node.

As a home agent, it MUST set the 'A' bit to '1', indicating this packet is coming from the home agent servicing this binding.

When a revocation message is being sent to a foreign agent, and the use of the 'I' bit was negotiated in the registration process, the home agent MUST set the 'I' bit to 1 if the home agent would like the foreign agent to inform the mobile node of the revocation. Conversely, if the home agent does not want the mobile node notified, it MUST set the 'I' bit to 0. Note that the home agent could also set the 'I' bit to '0' because it knows the mobile node has registered with a different foreign agent, and so there is no need for the foreign agent to attempt a notification.

The home agent MUST set the Identifier field as defined in Section 3.5., and MUST include a valid authenticator as specified in Section 3.3.

If the home agent does not receive a revocation acknowledgment message within a reasonable amount of time, it MUST retransmit the revocation message. How long the home agent waits to retransmit, and how many times the message is retransmitted is limited by the requirement that:

- every time the home agent is about to retransmit the revocation message, it MUST update the value of the timestamp in the revocation identifier with a current value from the same clock used to generate the timestamps in the revocation extensions sent to this foreign agent. Note that this also necessarily means updating any fields derived using the revocation identifier (e.g., a home-foreign authenticator).

- the home agent MUST NOT send more than one revocation per second for a particular binding,

- the time between retransmissions SHOULD fall-back in analogy with the registration guidelines in [1], namely exponential backoff, and

- the home agent MUST NOT retransmit revocation messages beyond the normal life of the binding identified by the revocation message.

4.2.2.2. Foreign Agent Responsibilities

Upon receiving a registration revocation message, the foreign agent MUST check that the validity of the authenticator, the 'A' bit, and the identifier field against replay as defined by Section 3.5. The foreign agent MUST also identify the binding described by the home agent as being released using the information in the revocation message, namely the addresses identified by the mobile node address, the foreign domain address, the home domain address, as well as the timestamp in the revocation message, and also the timestamp in the last accepted registration message; revocations are only valid for existing registrations, and so the timestamp of a registration MUST precede the revocation message (note that both of those timestamps were set by the same home agent). Upon locating the binding, the foreign agent MUST revoke it, and MUST respond with a revocation acknowledgment sent to the source address of the revocation message. If the 'I' bit was negotiated, the foreign agent MUST check the value of the 'I' bit in the revocation message and act accordingly.

If notifying the mobile node by the methods described in Section 4.1., the foreign agent MUST set the 'I' bit to '1' in the revocation acknowledgment to be sent to the home agent, or if not notifying the mobile node, the foreign agent MUST set the 'I' bit to '0'.

The foreign agent may discontinue all Mobile IP services by the former binding at this time, and free up any resources that were being used by it.

The foreign agent MUST then generate a revocation acknowledgment, setting the Home Address and Identifier field in the revocation acknowledgment message as described by Section 3.5., and protect it with a valid authenticator as specified in Section 3.3.

4.2.2.3. 'Direct' co-located mobile node Responsibilities

Upon receiving a revocation message, the 'direct' co-located mobile node MUST validate the authenticator, and check the home address and identifier specified in the revocation message for replay. If the packet passes authentication, and the identifier reveals this revocation to be new, the mobile node MUST verify that the information contained in the revocation messages identifies the home

agent with which it has a current binding, that this binding identifies correctly this mobile node and any foreign domain address it is currently using. If the mobile node is able to identify such a binding, the mobile node SHOULD first generate a revocation acknowledgment message which MUST be sent to the IP source address of the revocation message. The mobile node may then terminate any reverse tunnel encapsulation [C] it is using to this home agent, and consider its binding revoked, and free up any other resources associated with the former binding.

4.2.3. Foreign Domain Revoking/Releasing a Registration

The following section details the responsibilities of each party depending on the functionality negotiated in the revocation support extensions when the foreign domain is revoking a registration. Note that revocation support for a co-located mobile node registering via a foreign agent (because the 'R' bit was set in the agent's advertisement) is not supported. See Section 4.3.1. for details.

4.2.3.1. Foreign Agent Responsibilities

If the use of the 'I' bit was negotiated, and the foreign domain policy of informing the mobile node has not changed since the last successful registration exchange, the foreign agent MUST NOT inform any mobile node of its revocation at this time. Instead, the foreign agent MUST set the 'I' bit to '1' in the revocation message, thereby asking the home agent to use the 'I' bit in the revocation acknowledgment to indicate if it should notify the effected mobile nodes. If the policy on the foreign domain was to not notify the mobile node, or if it has changed since the most recent successful registration, and the foreign agent is no longer able to use the 'I' bit, the foreign agent MUST set the 'I' bit to '0', and follow the policies of the foreign domain with regard to notifying the mobile node.

Note that the 'A' bit MUST be set to '0' to indicate that the revocation message is coming from the foreign agent servicing this binding.

Before transmitting the revocation message, the foreign agent MUST set the revocation identifier as described by section 3.5., and MUST include an authenticator as described by section 3.3.

If the foreign agent does not receive a revocation acknowledgment message within a reasonable amount of time, it MUST retransmit the revocation message. How long the foreign agent waits to retransmit, and how many times the message is retransmitted is only limited by the following specifications:

- every time the foreign agent is about to retransmit the revocation message, it MUST update the value of the timestamp in the revocation identifier with a current value from the same clock used to generate the timestamps in the revocation extensions sent to this home agent. Note that this also necessarily means updating any fields derived using the revocation identifier (e.g., a home-foreign authenticator).

- MUST NOT send more than one revocation per second for a particular binding,

- SHOULD set its retransmissions to fall-back in analogy with the registration guidelines in [1], namely exponential backoff, and

- MUST NOT retransmit revocation messages beyond the normal life of the binding identified by the revocation message.

4.2.3.2. Home Agent Responsibilities

Upon receiving a registration revocation message, the home agent MUST check the 'A' bit, and identifier field, as well as the authenticator. If the packet is acceptable, the home agent MUST locate the binding identified by the foreign agent as being released using the information in the revocation message, namely the addresses identified by the home address, the foreign domain address and the home domain address fields. As revocations are only valid for existing registrations, the timestamp of a registration MUST precede the revocation message (note that both of those timestamps were set by the same foreign agent). Since this binding is no longer active, the home agent can free up any resources associated with the former binding and discontinue all Mobile IP services for it.

Upon processing a valid registration revocation message, the home agent MUST send a revocation acknowledgment to the IP source address of the registration revocation message.

If use of the 'I' bit was negotiated, and the 'I' bit is set to '1' in the revocation message, the home agent should decide if it wants the mobile node informed of the revocation of this binding. If it does want the mobile node informed, it MUST set the 'I' bit in the revocation acknowledgment message to '1'. If it does not want the mobile node informed, it MUST set the 'I' bit to '0'.

The home agent MUST set the Home Address, and Revocation Identifier fields as described by Section 3.5., and protect the revocation acknowledgment message with a valid authenticator as specified in Section 3.3.

4.2.4. Mobile Node Deregistering a Registration

The cases where a mobile node is registered with its home agent, whether it is registered directly with its home agent ('direct' co-located mobile node), or registered via a foreign agent, and wishes to terminate its own binding, the mobile node MUST NOT send a revocation message, but SHOULD simply deregister the appropriate care-of address with its home agent as described by [1].

4.3. Mobile IP Registration Bits in the Revocation Process

Several of the bits used in the registration process need special consideration when using the revocation mechanism.

4.3.1. The 'R' Bit in Use

If the foreign agent wishes to be able to revoke a mobile node's registration, it MUST set the 'R' bit in its agent advertisements. (A foreign agent advertising the 'R' bit requests every mobile node, even one that is co-located (and whose registration would otherwise by-pass the foreign agent), to register with the foreign agent.) However, in this case, the foreign agent SHOULD deny a registration request as "Administratively Prohibited" from a mobile node that is registering in a co-located fashion. The reason being that the foreign agent will not be able to revoke the binding of a co-located mobile node due to reasons outlined in Section 4.3.2.

How the foreign agent and/or foreign domain enforce the 'R' bit is beyond the scope of this document.

4.3.2. The 'D' bit in Use

A mobile node registering directly with its home agent in a co-located fashion with the 'D' bit set in its registration request is supported in registration revocation. However, support for a co-located mobile node (with the 'D' bit set in its registration request) registering via a foreign agent is not supported for the following reasons.

Registration requests where the 'D' bit is set, and which are relayed through a foreign agent (e.g., due to the advertising of the 'R' bit) should theoretically contain the foreign agent address as the source address of the registration request when received by the home agent. A home agent may conclude that the source address of this registration request is not the same as the co-located care-of address contained in the registration request, and is therefore likely to be the address of the foreign agent. However, since there is no way to guarantee that this IP source address is in fact an

address of the foreign agent servicing the mobile node, accepting a revocation message from this IP source address may lead to a denial-of-service attack by a man-in-the-middle on the mobile node.

Moreover, there is currently no method for the foreign agent servicing the mobile node to identify itself to the home agent during the Mobile IP registration phase. Even if a foreign agent could identify itself, the co-located mobile node would also need to authorize that this foreign agent is indeed the agent that is providing it the Mobile IP services. This is to thwart a denial-of-service attack on the mobile node by a foreign agent that has a security association with the home agent, and is on the path between the co-located mobile node and the home agent.

5. Error Codes

As the intent of a registration revocation message is not a request to discontinue services, but is a notification that Mobile IP services are discontinued, there are no new error codes.

6. Security Considerations

There are two potential vulnerabilities, one in the agent advertisement mechanism, and one related to unauthorized revocation messages.

6.1. Agent Advertisements

Although the mechanisms defined by this document do not introduce this problem, it has been recognized that agent advertisements as defined in [1] subject mobile nodes to a denial-of-service potential. This is because the agent advertisement as defined in [1] may be spoofed by other machines residing on the link. This makes it possible for such nodes to trick the mobile node into believing its registration has been revoked either by unicasting an advertisement with a reset sequence number to the link-local address of the mobile node, or by broadcasting it to the subnet, thereby tricking all mobile nodes registered with a particular foreign agent into believing all their registrations have been lost.

There has been some work in this working group and others (e.g., IPsec) to secure such router advertisements, though at the time of this publication, no solutions have become common practice. To help circumvent possible denial of service issues here, bringing their potential for disruption to a minimum, mobile node implementors should ensure that any agent advertisement which doesn’t conform to a strict adherence to [1], specifically those whose TTL is not 1, or which do not emanate from the same link-address (when present) as

other agent advertisements supposedly from the same agent, or even that of the last successful registration reply, be silently discarded.

6.2. Revocation Messages

As registration revocation, when performed, terminates Mobile IP services being provided to the mobile node, it is crucial that all security and replay protection mechanisms be verified before a mobility agent believes that the other agent has revoked a binding. Messages which are sent link-local (e.g., between mobile node and foreign agent) MAY also be secured by methods outlined in [1], namely the use of mobile-foreign authenticators, but these have no direct relation to registration revocation.

RFC 3344 [1] defines a security mechanism that MUST be used between home agents and mobile nodes, and MAY used between home agents and foreign agents, namely the use of authenticators. All foreign and home agents MUST support protection of revocation messages via the foreign-home authenticators defined in [1]. They MAY implement other mechanisms of equal or greater strength; if such mechanisms are known to be available to both parties, they MAY be used instead.

Revocation messages are at least as secure as registration messages passed between home and foreign agents and containing home-foreign authenticators as defined in [1]. Thus, there are no new security threats introduced by the revocation mechanism other than those present in [1] with respect to the compromise of the shared secret which is used to generate the home-foreign authenticators.

That said, there are two types of active attacks which use messages captured "in flight" by a man-in-the-middle between the home and foreign agents - "malicious repeaters" and "malicious reflectors".

In the case of a "malicious repeater", a man-in-the-middle captures a revocation message, then replays it to the same IP destination address at a later time. Presuming the authenticator of the original packet was deemed valid, without replay protection, the home-foreign authenticator of the replayed packet will (again) pass authentication. Note that since datagrams are not guaranteed to arrive unduplicated, a replay may occur by "design".

In the case of a "malicious reflector," a man-in-the-middle captures a revocation message, then returns it to its originator at a later time. If the security association between home and foreign domains uses a security association involving a (single) shared secret which only protects the contents of the UDP portion of the packet (such as home-foreign authenticators as defined by [1]), without replay

protection, the sender of the packet will also believe the revocation message to be authentic.

The replay protection mechanism used by the revocation messages defined by this document is designed to protect against both of these active attacks. As a benefit, by using a 32-bit timestamp it can be more quickly determined if revocation messages are replays, though the reader is advised to use caution in this approach. An agent which receives an authenticated revocation message can compare the Identifier field to that of a previously received revocation message, and if the timestamp in the new message is found to have been generated after that of the time-stamp in the last revocation message received, it can immediately be determined as not being a replay. Note however that since datagrams are not guaranteed to arrive in order, it should not be presumed that because the values contained in an Identifier field are timestamps that they will necessarily be increasing with each successive revocation message received. Should an implementor decide to base his replay detection mechanism on increasing timestamps, and therefore increasing Identifier values, a suitable time window should be defined in which revocation messages can be received. At worst, ignoring any revocation message should result in the retransmission of another revocation message, this time with timestamp later than the last one received.

Note that any registration request or reply can be replayed. With the exchanging of time-stamps by agents in revocation extensions, an agent should have a belief that such messages have been delivered in a timely manner. For purposes of registration revocation, the timeliness of a registration packet is simply based on the granularity of each registration. Since [1] provides a replay mechanism for the home agent to use, it has a way to tell if the registration request being presented to it is new. The foreign agent, however, has no such mechanism in place with the mobile node. Foreign agents are advised to continue to consider registrations 'outstanding' until the associated registration reply is returned from the home agent before using the information in any of its visitor entries. Even so, this leaves the foreign agent open to a potential denial of service attack in which registration requests and replies are replayed by multiple nodes. When this happens, the foreign agent could be lead to believe such registrations are active, but with old information, which can have adverse effects on them, as well as to the ability of that agent to successfully use the procedures outlined in this document. Sufficient protection against this scenario is offered by the challenge-response mechanism [2] by which a foreign agent generates a live challenge to a mobile node for the purposes of making sure, among other things, that the registration request is not a replay.

7. IANA Considerations

This document defines an additional set of messages between the home and foreign agent specific to the services being provided to the same mobile node, or sub-set of mobile nodes. To ensure correct interoperation based on this specification, IANA has reserved values in the Mobile IP number space for two new message types, and a single new extension.

7.1. New Message Types

The following message types are introduced by this specification:

Registration Revocation: A new Mobile IP control message, using UDP port 434, type 7. This value has been taken from the same number space as Mobile IP Registration Request (Type = 1), and Mobile IP Registration Reply (Type = 3).

Registration Revocation Acknowledgment: A new Mobile IP control message, using UDP port 434, type 15. This value has been taken from the same number space as Mobile IP Registration Request (Type = 1), and Mobile IP Registration Reply (Type = 3).

7.2. New Extension Values

The following extensions are introduced by this specification:

Revocation Support Extension: A new Mobile IP Extension, appended to a Registration Request, or Registration Reply. The value assigned is 137. This extension is derived from the Extension number space. It MUST be in the 'skippable' (128 - 255) range as defined in RFC 3344.

7.3. New Error Codes

There are no new Mobile IP error codes introduced by this document.

8. References

8.1. Normative References (Numerical)

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

[2] Perkins, C. and P. Calhoun, "Mobile IPv4 Challenge/Response Extensions", RFC 3012, November 2000.

[3] Bradner, S., "Key Words for us in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informational References (Alphabetical)

[A] Glass, S., Hiller, T., Jacobs, S. and C. Perkins, "Mobile IP Authentication, Authorization, and Accounting Requirements", RFC 2977, October 2000.

[B] Aboba, B., Calhoun, P., Glass, S., Hiller, T., McCann, P., Shiino, H., Walsh, P., Zorn, G., Dommety, G., Perkins, C., Patil, B., Mitton, D., Manning, S., Beadles, M., Chen, X., Sivalingham, S., Hameed, A., Munson, M., Jacobs, S., Lim, B., Hirschman, B., Hsu, R., Koo, H., Lipford, M., Campbell, E., Xu, Y., Baba, S. and E. Jaques, "Criteria for Evaluating AAA Protocols for Network Access", RFC 2989, November 2000.

[C] Montenegro, G., Ed., "Reverse Tunneling for Mobile IP, revised", RFC 3024, January 2001.

[D] Deering, S., Ed., "ICMP Router Discovery Messages", RFC 1256, September 1991.

[E] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", RFC 2794, March 2000.

Appendix A: An Example of the Revocation Messages in Use

For clarity, the following example is meant to illustrate the use of the new messages in the registration phase, and the revocation phase. In this example, a foreign agent and home agent will negotiate revocation during the registration phase. During the revocation phase, the foreign agent will revoke the binding of a mobile node.

A.1. The Registration Phase

Consider a foreign agent that supports registration revocation, and has a security association with a home agent to which it is forwarding a registration request. The foreign agent will include the revocation support extension after the mobile-home authenticator. Assume that the foreign agent supports the use of the 'I' bit, and is willing to let the home agent decide if the mobile node should be informed of the revocation of its registration. Thus, the foreign agent will set the 'I' bit to '1'. The foreign agent will append a foreign-home authenticator to the registration request.

Upon receiving the registration request containing a revocation extension, the home agent will include a revocation support extension in the registration reply. Since the foreign agent set the 'I' bit to '1' in its revocation extension, and the home agent supports the use of the 'I' bit, the home agent will set the 'I' bit in its registration extension to '1'. Additionally, the home agent will append a home-foreign authenticator to the registration request.

Upon receiving the authenticated registration reply, the foreign agent will check the revocation support extension and note that the home agent wants to decide if the mobile node should be notified in the event this registration is revoked, i.e., since the home agent set the 'I' bit in the return revocation extension.

A.2. The Revocation Phase

The foreign agent revokes a mobile node's binding, and generates a revocation message to be sent to the mobile node's home agent. Since the 'I' bit was negotiated in the revocation extensions, and the foreign agent is still willing to let the home agent indicate whether this mobile node should be informed about the revocation, it will set the 'I' bit to '1' in the revocation message. The foreign agent also makes sure the 'A' bit is set to '0'.

The foreign agent will also place the address of the mobile node whose registration it wishes to revoke in the home address field, the address that the mobile node registered as the care-of address in the foreign domain field, and the address registered as the home agent in

the home domain address field. The foreign agent will set the Revocation Identifier to the current 32-bit timestamp, and append the foreign-home authenticator.

Upon receiving the above revocation message, the home agent uses the address identified as the foreign domain address to identify the security association, and authenticate the revocation message. After authenticating the message, the home agent will check to make sure the 'A' bit and Identifier indicate that this revocation is not a replay. The home agent then uses the mobile node home address, foreign domain address, and home domain address to locate the mobile node whose registration is being revoked.

Upon processing a valid registration revocation message, the home agent generates a revocation acknowledgment message. Since the 'I' bit was set to '1' in the revocation message and the home agent wishes for the identified mobile node to be informed of the revocation, it will set the 'I' bit in the revocation acknowledgment to '1'. The home agent then copies the home address and the Revocation Identifier field into the revocation acknowledgement. The home agent protects the revocation acknowledgment with a home-foreign authenticator.

Upon receiving a valid revocation acknowledgment (in which the authenticator and Identifier fields are acceptable), the foreign agent checks the state of the 'I' bit. Since the 'I' bit is set to '1', the foreign agent will notify the mobile node of the revocation.

Appendix B: Disparate Address, and Receiver Considerations

Since the registration revocation message comes from a source address that is topologically routable from the interface receiving the datagram, the agents, by definition, are topologically connected (if this were not the case, the initial registration mechanism would have failed). If either are the ultimate hop from this topologically connected region to one or more disparate address spaces, no problems are foreseen. In order for the mobile node to have successfully registered with its home agent, it MUST have provided to the network (foreign agent) to which it is currently attached a routable address of its home agent. Conversely, the care-of address being used by the mobile node must also be topologically significant to the home agent in order for the registration reply to have been received, and the tunnel initiated. By definition, then, the home agent address and the care-of address must each be significant, and either address must form a unique pair in the context of this mobile node to both agents.

Another way of understanding this is that the tunnel endpoints are in some way connected, and hence each are unique as far as the other end is concerned. The address at the other end of the tunnel, in combination with the address of the mobile node, must therefore form a unique pair that can be identified by the agent receiving the registration revocation message.

As an example, consider a mobile node who's home address lies in disparate address space A behind its home agent. In the following diagram, [*] indicates an interface of the entity in which it appears.

```
   MN[a]-----[c]FA[b]=====((()))=====[b]HA[a]-----[a]CN

       Address      Some topologically      Address
       Space C      connected network       Space A
```

We presume a binding for MN exists, and hence a tunnel between FA[b] and HA[b] exists. Then, since the address assigned to MN[a] MUST be unique in address space A, the pair {FA[b],MN[a]} is guaranteed to be unique in the binding table of HA, and the pair {HA[b],MN[a]} is guaranteed to be unique in the foreign agent's visitor list.

As a result, a home agent receiving a registration revocation message and foreign-home authenticator for MN[a] from FA[b] is able to determine the unique mobile node address being deregistered. Conversely a foreign agent receiving a registration revocation message and home-foreign authenticator for MN[a] from HA[b] is able to determine the exact mobile node address being deregistered. For this reason, if a foreign agent receives a registration revocation message with the home domain field set to the zero address it MUST be silently discarded. This is to prevent confusion in the case of overlapping private addresses; when multiple mobile nodes are registered via the same care-of address and coincidentally using the same (disparate/private) home address, the home agent address appearing in the home domain field is the only way a foreign agent can discern the difference between these mobile nodes.

Acknowledgments

The authors would like to thank Rajesh Bhalla, Kent Leung, and Alpesh Patel for their contributions to the concepts detailed in draft-subbarao-mobileip-resource-00.txt, "Releasing Resources in Mobile IP," from which the revocation support extension, and the acknowledgment mechanism contained in this document were derived.

The authors would also like to thank Pete McCann for his discussions on replay mechanisms, and security concerns, and Ahmad Muhanna for pointing out a problem with the initial replay mechanism, which eventually lead to the addition of a time stamp to the Revocation Extension.

The authors would also like to acknowledge Henrik Levkowetz for his detailed review of the document, and Michael Thomas for his review of the replay mechanism described herein.

Authors' Addresses

Steven M. Glass
Solaris Network Technologies
Sun Microsystems
1 Network Drive
Burlington, MA. 01801

Phone: +1.781.442.0000
Fax: +1.781.442.1706
EMail: steven.glass@sun.com

Madhavi W. Chandra
IOS Technologies Division
Cisco Systems
7025 Kit Creek Road
Research Triangle Park, NC 27709

Phone: +1.919.392.8387
EMail: mchandra@cisco.com

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.