IETF Mobile IP Working Group
INTERNET DRAFT

Charles E. Perkins
Nokia Research Center
20 September 2005

Foreign Agent Error Extension for Mobile IPv4
draft-ietf-mip4-faerr-02.txt

Status of This Memo

This document is a submission by the IETF MIPv4 Working Group Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the mip4@ietf.org mailing list.

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Abstract

This document specifies a new extension for use by Foreign Agents operating Mobile IP for IPv4. Currently, a foreign agent cannot supply status information without destroying the ability for a mobile node to verify authentication data supplied by the home agent. The new extension solves this problem by making a better place for the foreign agent to provide its status information to the mobile node.

1. Introduction

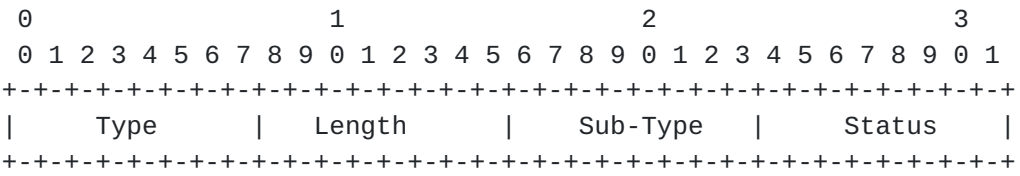
This document specifies a new non-skippable extension for use by Foreign Agents operating Mobile IP for IPv4 [4]. The new extension option allows a foreign agent to supply an error code without disturbing the data supplied by the Home Agent within the Registration Reply message. In this way, the mobile node can verify that the Registration Reply message was generated by the Home Agent even in cases where the foreign agent is required by protocol to insert new status information into the Registration Reply message.

2. Terminology

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 RFC 2119 [1]. Other terminology is used as already defined in [4].

3. FA Error Extension Format

The format of the FA Error Extension conforms to the Short Extension format specified for Mobile IPv4 [4]. The FA Error Extension is not skippable.



Type

<To Be Assigned by IANA>

Length

2

Sub-Type

0

Status

A status code used by the foreign agent to supply status information to the mobile node.

4. Operation and Use of the FA Error Extension

The FA Error extension is only valid for use within Mobile IPv4 Registration Reply messages. The FA Error Extension is not skippable. A mobile node that cannot correctly interpret the contents of the FA Error Extension MUST NOT use the care-of address provided in the Registration Reply message, until another Registration Request message has been sent and a successful Registration Reply message received.

Status codes allowable for use within the FA Error Extension are within the range 64-127. The currently specified codes are as follows:

64 reason unspecified
65 administratively prohibited
66 insufficient resources
68 home agent failed authentication
71 poorly formed Reply
77 invalid care-of address
78 registration timeout

as defined in RFC 3344 [4] for use by the Foreign Agent. Status codes for use with the FA Error extensions must not be differently defined for use in the Code field of Registration Reply messages.

When a foreign agent appends a FA Error Extension to the Registration Reply as received from the Home Agent, it has to update the UDP Length field in the UDP header [5] to account for the extra 4 bytes of length.

This document updates the Mobile IP base specification [4] regarding the procedures followed by the foreign agent in the case that the home agent fails authentication. Instead of modifying the "status" field of the Registration Reply to contain the value 68, now the foreign agent should append the Foreign Agent Error Extension containing the status value 68.

5. Mobile Node Considerations

If a mobile node receives a successful Registration Reply (status code 0 or 1), with a FA Error extension indicating that the foreign agent is not honoring said Registration Reply, the mobile node SHOULD then send a deregistration message to the home agent. In this way, the home agent will not maintain a registration status that is inconsistent with the status maintained by the foreign agent.

6. Foreign Agent Considerations

When denying a successful Registration Reply, the Foreign Agent SHOULD send the a Registration Revocation message [2] to the Home Agent if a mobility security association exists between them. For cases when the foreign agent does have the required security association, this way of informing the home agent does not have the vulnerability from detrimental actions by malicious foreign agents as noted in section 8.

7. IANA Considerations

This specification reserves one number for the FA Error extension (see section 3) from the space of numbers for non-skippable mobility extensions (i.e., 0-127) defined in the specification for Mobile IPv4 [4].

This specification also creates a new number space of sub-types for the type number of this extension. Sub-type zero is to be allocated from this number space for the protocol extension specified in this document. Similar to the procedures specified for Mobile IP [4] number spaces, future allocations from this number space require expert review[3].

The status codes which are allowable in the FA error extension are a subset of the status codes defined in the specification for Mobile IPv4 [4]. If, in the future, additional status codes are defined for Mobile IPv4, the definition for each new status code must indicate whether or not the new status code is allowable for use in the FA Error extension.

8. Security Considerations

The extension in this document improves the security features of Mobile IPv4 by allowing the mobile node to be assured of the authenticity of the information supplied within a Registration Request. Previously, whenever the foreign agent was required to provide status information to the mobile node, it could only do so by destroying the ability of the mobile device to verify the Mobile-Home Authentication Extension data.

In many common cases, the mobile node will not have a security association with the foreign agent that has sent the extension. Thus, the mobile node will be unable to ascertain that the foreign agent sending the extended Registration Reply message is the same foreign agent that earlier received the associated Registration Request from the mobile node. Because of this, a malicious foreign

agent could cause a mobile node to operate as if the registration had failed, when in fact its home agent and a correctly operating foreign agent had both accepted the mobile node's Registration Request. In order to reduce the vulnerability to such maliciously transmitted Registration Reply messages with the unauthenticated extension, the mobile node MAY delay processing of such denied Registration Reply messages for a short while in order to determine whether another successful Registration Reply might be received from the foreign agent.

9. Acknowledgements

Thanks to Kent Leung and Henrik Lefkowetz for suggested improvements to this specification.

References

[1] S. Bradner. Key words for use in RFCs to Indicate Requirement Levels. RFC 2119, Internet Engineering Task Force, March 1997.

[2] S. Glass and Madhavi Chandra. Registration Revocation in Mobile IPv4. RFC 3543, Internet Engineering Task Force, August 2003.

[3] T. Narten and H. Alvestrand. Guidelines for Writing an IANA Considerations Section in RFCs. RFC 2434, Internet Engineering Task Force, October 1998.

[4] Charles E. Perkins. IP Mobility Support for IPv4. RFC 3344, Internet Engineering Task Force, August 2002.

[5] J. B. Postel. User Datagram Protocol. RFC 768, Internet Engineering Task Force, August 1980.

All references are normative.

Author Address

Questions about this memo can be directed to the author:

Charles E. Perkins
Networking Technology Lab
Nokia Research Center
313 Fairchild Drive

Mountain View, California 94043
USA
Phone: +1-650 625-2986
Fax: +1 650 625-2502
EMail: charles.perkins@.nokia.com

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.