Network Working Group
Request for Comments: 4636
Category: Standards Track

C. Perkins
Nokia Research Center

October 2006

Foreign Agent Error Extension for Mobile IPv4

Status of This Memo

Copyright Notice

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

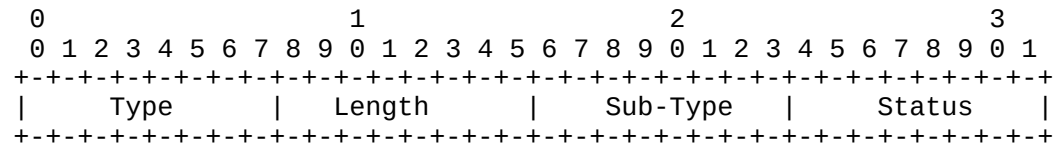
This document specifies a new non-skippable extension for use by Foreign Agents operating Mobile IP for IPv4 [4]. The new extension option allows a foreign agent to supply an error code without disturbing the data supplied by the Home Agent within the Registration Reply message. In this way, the mobile 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

45

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 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 that 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 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.

10. Normative References

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

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

[3] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

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

[5] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

Author's Address

Charles E. Perkins
Palo Alto Systems Research Lab
Nokia Research Center
975 Page Mill Road, Suite 200
Palo Alto, CA 94304-1003

Phone: +1 650-496-4402
Fax: +1-650-739-0779
EMail: charles.perkins@nokia.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).