Network Working Group
Request for Comments: 5094
Category: Standards Track

V. Devarapalli
Azaire Networks
A. Patel
K. Leung
Cisco

December 2007

Mobile IPv6 Vendor Specific Option

Status of This Memo

Copyright Notice

Abstract

There is a need for vendor-specific extensions to Mobility Header messages so that Mobile IPv6 vendors are able to extend the protocol for research or deployment purposes. This document defines a new vendor-specific mobility option.

Table of Contents

1. Introduction

Vendor-specific messages have traditionally allowed vendors to implement extensions to some protocols and distinguish themselves from other vendors. These messages are clearly marked by a Vendor ID that identifies the vendor. A particular vendor's implementation identifies the vendor extension by recognizing the Vendor ID. Implementations that do not recognize the Vendor ID either discard or skip processing the message.

Mobile IPv6 [2] is being deployed and there is a need for vendor-specific extensions to Mobility Header messages so that vendors are able to extend the Mobile IPv6 protocol for research or deployment purposes.

This document defines a new mobility option, the Vendor-Specific Mobility Option, which can be carried in any Mobility Header message. The Vendor-Specific mobility option MUST be used only with a Mobility Header message. Mobility options, by definition, can be skipped if an implementation does not recognize the mobility option type [2].

The messages defined in this document can also be used for NEMO [3] and Proxy MIPv6 [4] since these protocols also use Mobility Header messages.

Vendor-specific protocol extensions can cause serious interoperability issues and may in addition have adverse operational impact, if they are not designed and used carefully. The vendor-specific option described in this document is meant to support simple use cases where it is sufficient to include some vendor data in the standardized Mobile IPv6 protocol exchanges. The vendor-specific option is not suitable for more complex vendor extensions that modify Mobile IPv6 itself. Although these options allow vendors to piggyback additional data onto Mobile IPv6 message exchanges, RFC 3775 [2] requires that unrecognized options be ignored and that the end systems be able to process the remaining parts of the message correctly. Extensions that use the vendor-specific mobility option should require an indication that the option was processed, in the response, using the vendor-specific mobility option.

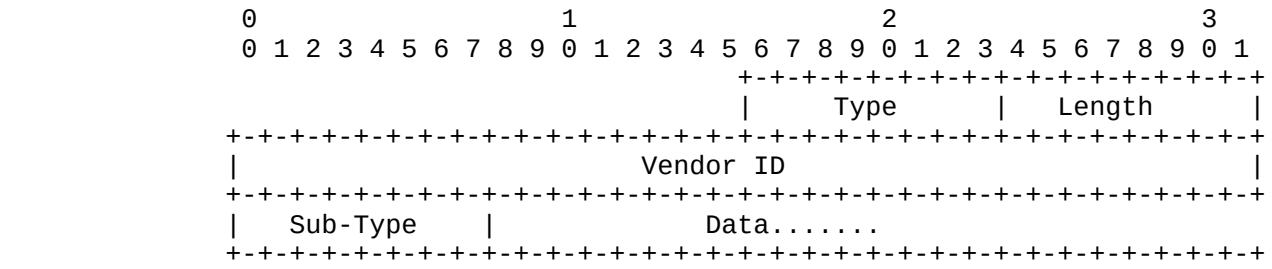
Vendors are generally encouraged to bring their protocol extensions to the IETF for review and standardization. Complex vendor extensions that modify Mobile IPv6 itself, will see large-scale deployment or involve industry consortia, or other multi-vendor organizations MUST be standardized in the IETF. Past experience has shown that such extensions of IETF protocols are critically dependent on IETF review and standardization.

2. Terminology

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 [1].

3. Vendor-Specific Mobility Option

The Vendor Specific Mobility Option can be included in any Mobility Header message and has an alignment requirement of 4n+2. If the Mobility Header message includes a Binding Authorization Data option [2], then the Vendor Specific mobility option should appear before the Binding Authorization Data option. Multiple Vendor-Specific mobility options MAY be present in a Mobility Header message.



Type

An 8-bit field indicating that it is a Vendor-Specific mobility option.

Length

An 8-bit field indicating the length of the option in octets excluding the Type and the Length fields. All other fields are included.

Vendor ID

The SMI Network Management Private Enterprise Code of the IANA-maintained Private Enterprise Numbers registry [5].

Sub-type

An 8-bit field indicating the type of vendor-specific information carried in the option. The administration of the Sub-type is done by the Vendor.

Data

Vendor-specific data that is carried in this message.

4. Security Considerations

The Vendor-Specific mobility messages should be protected in a manner similar to Binding Updates and Binding Acknowledgements if it carries information that should not be revealed on the wire or that can affect the binding cache entry at the home agent or the correspondent node. In particular, the messages containing the Vendor Specific mobility option MUST be integrity protected.

5. IANA Considerations

The Vendor-Specific mobility option, defined in Section 3, has been assigned the type value (19), allocated from the same space as the Mobility Options registry created by RFC 3775 [2].

6. Acknowledgements

The author would like to thank Jari Arkko and Basavaraj Patil with whom the contents of this document were discussed first.

7. References

7.1. Normative References

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

[2] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

7.2. Informative References

[3] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[4] Gundavelli, S., "Proxy Mobile IPv6", Work in Progress, March 2007.

[5] IANA Assigned Numbers Online Database, "Private Enterprise Numbers", <http://www.iana.org/assignments/enterprise-numbers>.

Authors' Addresses

Vijay Devarapalli
Azaire Networks
3121 Jay Street
Santa Clara, CA 95054
USA

EMail: vijay.devarapalli@azairenet.com

Alpesh Patel
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

EMail: alpesh@cisco.com

Kent Leung
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

EMail: kleung@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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