Network Working Group
Request for Comments: 5149
Category: Informational

J. Korhonen
U. Nilsson
TeliaSonera
V. Devarapalli
Azaire

February 2008

Service Selection for Mobile IPv6

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

In some Mobile IPv6 deployments, identifying the mobile node or the mobility service subscriber is not enough to distinguish between multiple services possibly provisioned to the said mobile node and its mobility service subscription. A capability to specify different services in addition to the mobile node identity can be leveraged to provide flexibility for mobility service providers on provisioning multiple services to one mobility service subscription. This document describes a Service Selection Mobility Option for both conventional Mobile IPv6 and Proxy Mobile IPv6 that is intended to assist home agents to make a specific service selection for the mobility service subscription during the binding registration procedure.

Table of Contents

1. Introduction

Mobile IPv6 [2] can identify mobile nodes in various ways, including home addresses [2], Network Access Identifiers (NAIs) [6][7], and credentials suitable for the Internet Key Exchange Protocol version 2 (IKEv2) [10]. In some Mobile IPv6 deployments, identifying the mobile node or the mobility service subscriber via a Proxy Mobile IPv6 client [5] (hereafter, the mobile node and the Proxy Mobile IPv6 client are used interchangeably) is not enough to distinguish between multiple services possibly provisioned to the said mobile node and its mobility service subscription.

The capability to specify different services in addition to the mobile node identity can be leveraged to provide flexibility for mobility service providers to provide multiple services within the same mobility service subscription. For example:

- Provide an enterprise data access for which the mobility service provider hosts connectivity and mobility services on behalf of the enterprise.
- Provide access to service domains that are otherwise not accessible from public networks because of some mobility service provider's business reasons.
- Provide simultaneous access to different service domains that are separated based on policies of the mobility service provider.
- Enable easier policy and quality of service assignment for mobility service providers based on the subscribed services.
- In the absence of a specifically indicated service, the home agent MUST act as if the default service, plain Internet access, had been requested. There is no absolute requirement that this default service be allowed to all subscribers, but it is highly RECOMMENDED in order to avoid having normal subscribers employ operator-specific configuration values in order to get basic service.

This document describes a Service Selection Mobility Option for Mobile IPv6 that is intended to assist home agents to make specific service selections for the mobility service subscription during the binding registration procedure. The service selection may affect home agent routing decisions, Home Address or Home Network Prefix assignment policies, firewall settings, and security policies. The Service Selection option should be used in every Binding Update that makes a new registration to the home agent.

Some of the potential use-cases were listed earlier in this section. The general aim is better manageability of services and service provisioning from the point of view of both operators and service providers. However, it should be understood that there are potential deployment possibilities where selecting a certain service may restrict simultaneous access to other services from a user's point of view. For example, services may be located in different administrative domains or external customer networks that practice excessive filtering of inbound and outbound traffic.

2. Requirements

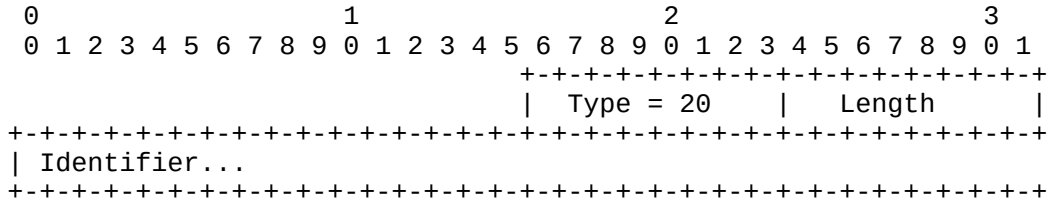
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [1].

3. Service Selection Mobility Option

At most one Service Selection Mobility Option MAY be included in any Binding Update message. If the Binding Update message includes any authorization-related options (such as the Binding Authorization Data option [2]) or authentication related options (such as the Mobility Message Authentication option [8]), then the Service Selection option MUST appear before any mobility message authorization- or authentication-related options.

The Service Selection option SHOULD NOT be sent to a correspondent node. The mobile node cannot assume that the correspondent node has any knowledge about a specific service selection made between the mobile node and the home agent.

The Service Selection option has no alignment requirement as such.



Service Selection Mobility Option

- Type: 8-bit identifier set to 20 of the type of the skipable mobility option.

- Length: 8-bit unsigned integer, representing the length of the Service Selection Mobility Option in octets, excluding the Option Type and Option Length fields. A value of zero (0) is not allowed.

- Identifier: A variable-length encoded service identifier string used to identify the requested service. The identifier string length is between 1 and 255 octets. This specification allows international identifier strings that are based on the use of Unicode characters, encoded as UTF-8 [3], and formatted using Normalization Form KC (NFKC) as specified in [4].

  'ims', 'voip', and 'voip.companyxyz.example.com' are valid examples of Service Selection option Identifiers. At minimum, the Identifier MUST be unique among the home agents to which the mobile node is authorized to register.

4. Processing Considerations

4.1. Mobile Node Considerations

A mobile node or a Proxy Mobile IPv6 client MAY include, at most, one Service Selection Mobility Option into a Binding Update message. The option is used to identify the service to be associated with the binding registration and SHOULD only be included into the initial Binding Update message sent to a home agent. If the mobile node wishes to change the selected service, it is RECOMMENDED that the mobile node de-register the existing binding with the home agent before proceeding with a binding registration for a different service. The provisioning of the service identifiers to the mobile node or to the Proxy Mobile IPv6 client is out of the scope of this specification.

The placement of the Service Selection option is as follows: when present, this option MUST appear after the Mobile Node-Network Access Identifier (MN-NAI) option, if the MN-NAI option is present, and before any authorization- and authentication-related options. The Service Selection option can be used with any mobile node identification method such as a home address, an MN-NAI, and credentials suitable for IKEv2.

If the mobile node receives a Binding Acknowledgement with a Status Code set to SERVICE_AUTHORIZATION_FAILED and the mobile node has an existing binding with the Home Address or the Home Network Prefix used in the failed Binding Update message, the mobile node MUST

delete the existing binding. If there is no existing binding, the mobile node proceeds as with any failed initial binding registration.

4.2. Home Agent Considerations

Upon receiving a Binding Update message with a Service Selection option, the home agent authenticates and authorizes the mobile node. If the home agent supports the Service Selection, it MUST also verify that the mobile node is authorized for the service it included in the Service Selection option. The services the mobile node is authorized for SHOULD be part of the general mobile node subscription profile. If the mobile node is not authorized for the service, the home agent MUST deny the registration and send a Binding Acknowledgement with a Status Code set to SERVICE_AUTHORIZATION_FAILED (151).

The Service Selection option is used to assist the authorization and identifies a specific service that is to be authorized. The Service Selection option MAY also affect the Home Address or the Home Network Prefix allocation when, for example, used with the MN-NAI option. For example, for the same NAI there MAY be different Home Addresses or Home Network Prefixes depending on the identified service. Furthermore, the Service Selection option MAY also affect the routing of the outbound IP packets in the home agent depending on the selected service. The home agent MAY also apply different policy or quality of service treatment to traffic flows based on the selected service.

If the newly arrived Binding Update message with a Service Selection option indicates a change in the selected service, then the home agent MUST re-authorize the mobile node. Depending on the home agent policies, the services policies, Home Address or Home Network Prefix allocation policies, and the subscription policies, the home agent may or may not be able to authorize the mobile node to the new service. For example, the existing service and the new service could require different Home Network Prefixes. If the authorization fails, then the home agent MUST deny the registration, delete any binding with the existing Home Address or Home Network Prefix, and send a Binding Acknowledgement with a Status Code set to SERVICE_AUTHORIZATION_FAILED (151).

4.3. Correspondent Node Considerations

Unless the correspondent node and the home agent share the same knowledge about mobility services, the Service Selection option is more or less useless information to the correspondent node. The correspondent node SHOULD silently ignore the Service Selection option in this case.

There are deployment cases where the home agent and a correspondent node, for example, belong to the same administrative domain. In this case, it is possible that the correspondent node shares the same knowledge of the services as the home agent. Therefore, the correspondent node is, for example, able to provide service-based traffic handling to mobile nodes.

5. Security Considerations

The protection for the Service Selection Mobility Option depends on the service that is being identified and eventually selected. If the service selection information should not be revealed on the wire, Binding Updates and Binding Acknowledgements should use Encapsulating Security Payload (ESP) [9] in transport mode with a non-null encryption transform to provide message confidentiality.

6. IANA Considerations

A new Mobile IPv6 Mobility Option type has been assigned for the following new mobility option described in Section 3:

Service Selection Mobility Option is set to 20

A new Mobile IPv6 registration denied by home agent Status Code has been assigned. The Status Code was allocated from the range 128-255:

SERVICE_AUTHORIZATION_FAILED is set to 151

7. Acknowledgements

Jouni Korhonen would like to thank the TEKES MERCoNe project for providing funding to work on this document. The authors would like to thank Jari Arkko for his thorough review.

8. References

8.1. 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.

[3] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, November 2003.

[4] Davis, M. and M. Duerst, "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.0.0, October 2006.

8.2. Informative References

[5] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", Work in Progress, December 2007.

[6] Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

[7] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.

[8] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Authentication Protocol for Mobile IPv6", RFC 4285, January 2006.

[9] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[10] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.

Authors' Addresses

Jouni Korhonen
TeliaSonera Corporation
P.O. Box 970
FIN-00051 Sonera
Finland

EMail: jouni.korhonen@teliasonera.com

Ulf Nilsson
TeliaSonera Corporation
Marbackagatan 11
S-123 86 Farsta
Sweden

EMail: ulf.s.nilsson@teliasonera.com

Vijay Devarapalli
Azaire Networks
4800 Great America Pkwy
Santa Clara, CA 95054
USA

EMail: vijay.devarapalli@azairenet.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.