

Network Working Group
Internet-Draft
Expires: August 11, 2005

A. Patel
K. Leung
Cisco Systems
M. Khalil
H. Akhtar
Nortel Networks
K. Chowdhury
Starent Networks
February 10, 2005

Mobile Node Identifier Option for Mobile IPv6
draft-ietf-mip6-mn-ident-option-02.txt

Status of this Memo

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with [RFC 3668](#).

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>.

This Internet-Draft will expire on August 11, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

Mobile IPv6 defines a new Mobility header which is used by mobile nodes, correspondent nodes, and home agents in all messaging related to the creation and management of bindings. Mobile IPv6 nodes need the capability to identify themselves using an identity other than

the default home IP address. Some examples of identifiers include NAI, FQDN, IMSI, MSISDN, etc. This document defines a new mobility option that can be used by Mobile IPv6 entities to identify themselves in messages containing a mobility header.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Mobile Node Identifier option	5
3.1	MN-NAI mobility option	6
3.2	Processing Considerations	6
4.	Security Considerations	7
5.	IANA Considerations	8
6.	Acknowledgements	9
7.	Normative References	9
	Authors' Addresses	9
	Intellectual Property and Copyright Statements	11

1. Introduction

The base specification of Mobile IPv6 [[RFC3775](#)] identifies mobility entities using an IPv6 address. It is essential to have a mechanism wherein mobility entities can be identified using other identifiers (for example, a network access identifier (NAI) [[RFC_2486bis](#)], International Mobile Station Identifier (IMSI), an application/deployment specific opaque identifier etc).

The capability to identify a mobility entity via identifiers other than the IPv6 address can be leveraged for performing various functions, eg.

- o authentication and authorization using an existing AAA (Authentication, Authorization and Accounting) infrastructure or via an HLR/AuC (Home Location Register/Authentication Center),
- o dynamic allocation of a mobility anchor point,
- o dynamic allocation of a home address etc.

This document defines an option with subtype number which denotes a specific type of identifier. One instance of subtype, the NAI is defined in [Section 3.1](#). It is anticipated that other identifiers will be defined for use in the mobility header in the future.

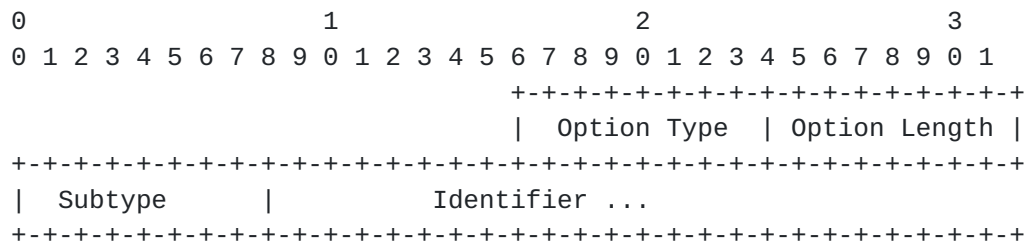
2. Terminology

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](#).

3. Mobile Node Identifier option

The Mobile node identifier option is a new optional data field that is carried in the Mobile IPv6 defined messages which includes the mobility header. Various forms of identifiers can be used to identify a MN. Some examples include a Network Access Identifier (NAI) [[RFC 2486bis](#)], an opaque identifier applicable to a particular application, etc. The subtype field in the option defines the specific type of identifier.

This option can be used in mobility messages containing a mobility header. The subtype field in the option is used to interpret the specific type of identifier.



Option Type:

MN-ID-OPTION-TYPE to be defined by IANA. An 8-bit identifier of the type mobility option.

Option Length:

8-bit unsigned integer, representing the length in octets of the Subtype and Identifier fields.

Subtype:

Subtype field defines the specific type of identifier included in the identifier field.

Identifier:

A variable length identifier of type as specified by the subtype field of this option.

This option does not have any alignment requirements.

[3.1](#) MN-NAI mobility option

The format of the MN-NAI mobility option is as defined in [Section 3](#). This option uses the subtype value of 1. The MN-NAI mobility option is used to identify the mobile node.

The MN-NAI mobility option uses an identifier of the form user@realm [[RFC 2486bis](#)].

[3.2](#) Processing Considerations

The location of the MN identifier option is as follows: When present, this option MUST appear before any authentication related option in a message containing a mobility header.

4. Security Considerations

Mobile IPv6 already contains one mechanism for identifying mobile nodes, the Home Address Option [[RFC 3775](#)]. As a result, the vulnerabilities of the new option defined in this document are similar to those that already exist for Mobile IPv6. In particular, the use of a permanent, stable identifier may compromise the privacy of the user, making it possible to track a particular device or user as it moves through different locations.

In addition, since an NAI reveals the home affiliation of a user, it may assist an attacker in determining the identity of the user, help the attacker in targeting specific victims, or assist in further probing of the username space.

These vulnerabilities can be addressed through various mechanisms, such as those discussed below:

- o Encrypting traffic at link layer such that other users on the same link do not see the identifiers. This mechanism does not help against attackers on the rest of the path between the mobile node and its home agent.
- o Encrypting the whole packet, such as when using IPsec to protect the communications with the home agent [[RFC 3776](#)].
- o Using an authentication mechanism that enables the use of privacy NAIs [[RFC 2486bis](#)] or temporary, changing "pseudonyms" as identifiers.

In any case, it should be noted that as the identifier option is only needed on the first registration at the home agent and subsequent registrations can use the home address, the window of privacy vulnerability in this document is reduced as compared to the [RFC 3775](#). In addition, this document is a part of a solution to allow dynamic home addresses to be used. This is an improvement to privacy as well, and affects both communications with the home agent and the correspondent nodes, both of which have to be told the home address.

5. IANA Considerations

IANA services are required for this document. The values for new mobility options must be assigned from the Mobile IPv6 [[RFC3775](#)] numbering space.

The values for Mobility Option types MN-ID-OPTION-TYPE as defined in [Section 3](#) need to be assigned. The suggested value is 7 for the MN-ID-OPTION-TYPE.

IANA should record a value for this new mobility option.

In addition, IANA needs to create a new namespace for the subtype field of the Mobile Node Identifier Option. The currently allocated values are as follows:

NAI (defined in this document)	[1]
--------------------------------	-----

New values for this namespace can be allocated using Standards Action [[RFC2434](#)].

6. Acknowledgements

The authors would like to thank Basavaraj Patil for his review and suggestions on this draft. Thanks to Jari Arkko for review and suggestions regarding security considerations and various other aspects of the document.

7 Normative References

- [RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [RFC3775] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", [RFC 3775](#), June 2004.
- [RFC_2486bis]
Aboba, et. al., B., "The Network Access Identifier",
[draft-ietf-radext-rfc2486bis-03.txt](#) (work in progress),
November 2004.

Authors' Addresses

Alpesh Patel
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US

Phone: +1 408-853-9580
EMail: alpesh@cisco.com

Kent Leung
Cisco Systems
170 W. Tasman Drive
San Jose, CA 95134
US

Phone: +1 408-526-5030
EMail: kleung@cisco.com

Internet-Draft Mobile Node Identifier Option for Mobile IPv6
February 2005

Mohamed Khalil
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972-685-0574
EMail: mkhalil@nortelnetworks.com

Haseeb Akhtar
Nortel Networks
2221 Lakeside Blvd.
Richardson, TX 75082
US

Phone: +1 972-684-4732
EMail: haseebak@nortelnetworks.com

Kuntal Chowdhury
Starent Networks
2540 Coolwater Dr.
Plano, TX 75025
US

Phone: +1 214 550 1416
EMail: kchowdury@starentnetworks.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.

Acknowledgment

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

