

Network Working Group
Request for Comments: 3846
Category: Standards Track

F. Johansson
ipUnplugged
T. Johansson
Bytemobile
June 2004

Расширение Mobile IPv4 для передачи идентификаторов доступа Mobile IPv4 Extension for Carrying Network Access Identifiers

Статус документа

Данный документ содержит спецификацию стандартного протокола Internet, предложенного сообществу Internet, и является приглашением к дискуссии в целях развития этого протокола. Сведения о текущем состоянии стандартизации протокола вы найдете в документе Internet Official Protocol Standards (STD 1). Документ можно распространять без ограничений.

Авторские права

Copyright (C) The Internet Society (2004).

Тезисы

При перемещении мобильного узла из одной сети в другую требуется повторная аутентификация этого узла. Если в домашней сети используется множество серверов AAA¹ и агентов HA² у сервера Home AAA может отсутствовать достаточная для корректной повторной аутентификации узла информация, что может привести к необходимости смены HA для узла. В настоящем документе определено расширение Mobile IP, используемое для передачи идентификаторов серверам Home AAA и HA в форме NAI³. Это расширение позволяет агентам HA передавать свою идентификационную информацию, а также данные о сервере Home AAA мобильному узлу, который может передать ее на локальный сервер AAA при изменении точки подключения. Это расширение может также использоваться в других ситуациях, требующих обмена NAI между узлами Mobile IP.

Оглавление

1. Введение.....	1
2. Спецификация требований.....	2
3. Расширение для передачи NAI.....	2
3.1. Обработка NAI Carrying Extension.....	2
4. Субтип HA Identity.....	2
5. Субтип AAAH Identity.....	3
6. Вопросы безопасности.....	3
7. Согласование с IANA.....	3
8. Благодарности.....	3
9. Нормативные документы.....	3
10. Адреса авторов.....	4
11. Полное заявление авторских прав.....	4
Интеллектуальная собственность.....	4
Подтверждение.....	4

1. Введение

При создании сетей одним из требований является обеспечение резервирования. Для решения этой задачи в одном домене может использоваться множество серверов AAA. Когда мобильный узел регистрируется в сети, процедура аутентификации выполняется с использованием одного из серверов AAA в домашнем домене пользователя. При последующей регистрации пользователя в другом домене процедура аутентификации должна повторяться. Однако избыточность, обеспечиваемая протоколом AAA, может привести к тому, что повторная аутентификация будет выполняться с использованием другого сервера AAAH, который может не иметь информации о присвоенной сессии HA. В этом документе определяется расширение протокола Mobile IP, которое может использоваться для распространения данных, позволяющих решить эту проблему. Более того, обычно единственной информацией о домашнем агенте (HA) в регистрационном запросе является адрес IP, как определено в RFC 3344 [5]. К сожалению этого может оказаться недостаточно для некоторых инфраструктур AAA (таких, как Diameter [6]), использующих маршрутизацию на базе областей (realm); таким инфраструктурам AAA требуется знать полное имя FQDN⁴ для домашнего агента, чтобы обеспечить корректную обработку. Просмотр обратной зоны DNS⁵ позволяет идентифицировать лишь интерфейс Mobile IP для IP-адреса HA, который может не обеспечивать взаимно-

¹Authentication Authorization and Accounting – аутентификация, авторизация (предоставление полномочий) и учет.

²Home Agent – домашний агент.

³Network Access Identifier – идентификатор доступа в сеть.

⁴Fully Qualified Domain Name.

⁵Reverse DNS lookup.

5. Субтип AAAH Identity

Для AAAH Identity используется субтип 2 расширения NAI Carrying Extension. Идентификация содержит NAI домашнего сервера AAA в формате `hostname@realm`. Имя хоста вместе с областью формируют полное имя FQDN (`hostname.realm`) для домашнего сервера AAA.

Если в домашней сети имеется несколько серверов AAA, домашний агент, обеспечивающий поддержку выбора AAAH, в соответствии с данным документом **должен** обеспечивать AAAH identity в первом сообщении Registration Reply, передаваемом мобильному узлу MN. Расширение требуется включать в последующие сообщения Registration Reply лишь в тех случаях, когда это же расширение было включено в сообщение Registration Request, полученное от того же узла MN.

Мобильному узлу **следует** сохранять последнюю идентификацию AAAH Identity, полученную в сообщении Registration Reply, а также **следует** включать AAAH Identity в каждое последующее сообщение Registration Request при повторной аутентификации в целях повышения эффективности. Невозможность доступа к указанному серверу AAAH при повторной аутентификации будет приводить к возврату нового значения AAAH Identity NAI (которое следует сохранить и включать в последующие регистрационные запросы). Отказ при аутентификации (например, в результате недоступности AAAH) будет приводить к разрыву сессии Mobile IP; при инициировании нового сеанса мобильному узлу может указываться новое значение AAAH для его использования после новой регистрации.

Чужому агенту, который получает AAAH NAI с этим расширением в регистрационном запросе, **следует** включить полученную идентификацию AAAH NAI при запросе аутентификации мобильного узла через инфраструктуру AAA, если используемый протокол AAA способен передать эту информацию.

6. Вопросы безопасности

Данная спецификация вводит новые расширения Mobile IP, используемые для передачи идентификации мобильного агента и сервера AAA в форме идентификаторов NAI. Сообщения Mobile IP, которые переносят такие расширения, **должны** аутентифицироваться, как указано в [4], если ранее не был согласован иной метод аутентификации. Следовательно, данная спецификация не снижает уровень защиты сообщений Mobile IP.

Следует отметить, что содержащаяся в описанных здесь расширениях идентификация **может** передаваться через сеть в открытом виде. Однако авторы не представляют себе, как это могло бы привести к проблемам безопасности.

7. Согласование с IANA

В этом документе определены новое расширение Mobile IP и новое пространство кодов субтипа расширений Mobile IP для управления IANA.

В главе 3 определено новое расширение Mobile IP - Mobile IP NAI Carrying Extension. Код типа для этого расширения - 136. Данное расширение добавляет новое пространство кодов субтипа, в котором значения 1 и 2 выделены настоящим документом. Рассмотрение новых кодов субтипа для Mobile IP NAI Carrying Extension выполняется в соответствии с процедурой Expert Review¹, и описывается при необходимости, как указано в документе [3].

Содержание и формат данного расширения не привязаны к конкретным AAA NAI, поэтому при определении в будущем новых значений NAI, которые не будут относиться к категории AAA NAI, они могут, тем не менее, быть согласованы с пространством кодов субтипа, определенным в данном документе для NAI Carrying Extension.

Для расширений NAI Carrying Extension следует выделять значения кодов типа одновременно из пространства IANA для необязательных (skippable) расширений Mobile IPv4 и пространства IANA для анонсов Mobile IPv4. В идеальном случае выделяемые из этих пространств значения должны совпадать.

8. Благодарности

Спасибо авторам исходного документа GNAIE - Mohamed M Khalil, Emad Qaddoura, Haseeb Akhtar и Pat R. Calhoun. Исходный документ был удален из "сферы влияния" рабочей группы MIP, поскольку она не использовала данное расширение. Идеи этого документа использованы здесь. Благодарим также Henrik Levkowetz и Kevin Purser за их полезные отклики и помощь в написании этого документа.

9. Нормативные документы

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), March 1997.
- [2] Aboba, B. and M. Beadles, "The Network Access Identifier", [RFC 2486](#), January 1999.
- [3] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, [RFC 2434](#), October 1998.
- [4] Calhoun, P. and C. Perkins, "Mobile IP Network Access Identifier Extension for IPv4", [RFC 2794](#), March 2000.
- [5] Perkins, C., "IP Mobility Support for IPv4", [RFC 3344](#), August 2002.
- [6] Calhoun, P., Loughney, J., Guttman, E., Zorn, G. and J. Arkko, "Diameter Base Protocol", RFC 3588, September 2003.

¹Рецензия эксперта.

10. Адреса авторов

Fredrik Johansson

ipUnplugged AB

Arenavagen 23

Stockholm S-121 28

SWEDEN

Phone: +46 8 725 5916

EMail: fredrik@ipunplugged.com

Tony Johansson

Bytemobile Inc

2029 Stierlin Court

Mountain View, CA 94043

USA

Phone: +1 650 862 0523

EMail: tony.johansson@bytemobile.com

Перевод на русский язык

Николай Малых

EMail: nmalykh@gmail.com

11. Полное заявление авторских прав

Copyright (C) The Internet Society (2004).

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/S HE 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.

Интеллектуальная собственность

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 IETF's procedures with respect to rights in IETF 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.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.