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 найдёте в документе Internet Official Protocol Standards (STD 1). Документ можно распространять без ограничений.

Авторские права

Аннотация

При перемещении мобильного узла из одной сети в другую требуется повторная аутентификация этого узла. Если в домашней сети используется множество серверов AAA[1] и агентов HA[2] 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 NAI[3]. Это расширение позволяет агентам HA передавать свою идентификационную информацию, а также данные о сервере Home AAA мобильному узлу, который может передать её 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

При создании сетей одним из требованием 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 FQDN[4] для домашнего агента, чтобы обеспечить корректную обработку. Просмотр обратной зоны DNS[5] позволяет идентифицировать лишь интерфейс Mobile IP для IP-адреса HA, который может не обеспечивать взаимно-однозначного соответствия с именем FQDN данного домашнего агента. Это является для HA основанием включать свою идентификацию в регистрационный отклик. Определённое в этом документе расширение MIP v4 включает также субтип, показывающий, как это можно сделать. Идентификация HA тогда может быть включена мобильным узлом в последующие регистрационные запросы через другие точки подключения.

[1]Authentication Authorization and Accounting - аутентификация, авторизация (предоставление полномочий) и учёт.
[2]Home Agent - домашний агент.
[3]Network Access Identifier - идентификатор доступа в сеть.
[4]Fully Qualified Domain Name.
[5]Reverse DNS lookup.

2. Спецификация требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с BCP 14, RFC 2119 [1].

Используемая в документе терминология, связанная с Mobile IP, описана в RFC 3344 [5]. В дополнение здесь определено ещё несколько используемых в данном документе терминов:

AAAH
Один из нескольких серверов AAA в домашней сети

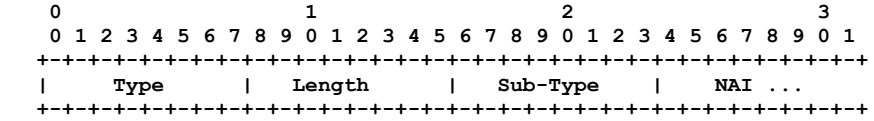
FQDN
Fully Qualified Domain Name - полное доменное имя, включающее имя хоста в домене и имя самого домена.

Identity
Идентификация узла, определяемая его FQDN.

NAI
Network Access Identifier - идентификатор доступа в сеть [2].

3. Расширение для передачи NAI

В этом документе описывается расширение NAI Carrying Extension, которое может использоваться в запросах и откликах Mobile IP Registration, а также в анонсах Mobile IP Agent [5]. Расширение может быть использовано любым узлом, которых хочет передать идентификацию в форме NAI [4]. В этом документе определены также несколько номеров субтипов, которые идентифицируют конкретные типы передаваемых NAI (главы 4 и 5). Предполагается, что дополнительные типы NAI будут определяться в последующих документах.



Type (тип) - 136 (может быть опущен) [5].

Length (размер) - 8-битовое целое число без знака. Задаёт размер расширения в октетах с учётом полей Type и Length. В это поле **должно** помещаться значение, на 1 превышающее общий размер поля NAI.

Sub-Type (субтип) - это поле показывает конкретный тип NAI, передаваемый в поле NAI.

NAI - значение NAI [2] в форме строки (string).

3.1. Обработка NAI Carrying Extension

Когда мобильный узел или домашний агент добавляет NAI Carrying Extension в регистрационное сообщение, это расширение **должно** размещаться до любых расширений, связанных с аутентификацией.

Если чужой агент (FA[1]) добавляет NAI Carrying Extension в регистрационное сообщение, это расширение **должно** появляться до любых связанных с аутентификацией расширений, добавляемых FA.

Если агент HA добавил NAI Carrying Extension в отклик Registration Reply для MN, и не получил расширение NAI в последующих сообщениях Registration Request от MN, этот агент HA может предполагать, что MN не понимает расширение NAI. В таких случаях агенту HA **не нужно** добавлять это расширение NAI в конце последующих сообщений Registration Reply, передаваемых MN.

4. Субтип HA Identity

Для HA Identity используется субтип 1 расширения NAI Carrying Extension. Идентификация содержит значение NAI для HA в форме hostname@realm. Имя хоста вместе с областью формируют полное имя FQDN (hostname.realm) для HA.

Домашний агент, использующий это расширение, **должен** обеспечить его присутствие в первом сообщении Registration Reply, передаваемом мобильному узлу MN[2], который в настоящее время не зарегистрирован. Расширение требуется включать в последующие сообщения Registration Reply лишь в тех случаях, когда это же было расширение включено в сообщение Registration Request, полученное от того же узла MN.

Мобильный узел, использующий это расширение, **должен** (если он получает это расширение в сообщении Registration Reply) включать его в каждый последующий регистрационный запрос, когда требуется повторная аутентификация. Отказ в повторной аутентификации (например, по причине недоступности AAAH) может приводить к прерыванию сеанса Mobile IP. При инициировании новой сессии мобильному узлу может передаваться новое значение HA Identity NAI и приведённые выше требования будут относиться к полученному в этом случае NAI.

Если мобильному узлу требует конкретный домашний агент и имеется NAI, узел **должен** обеспечить включение данного расширения в начальный регистрационный запрос.

Чужому агенту, который получил HA NAI с этим расширением в регистрационном запросе, **следует** включить HA NAI при запросе аутентификации MN через инфраструктуру AAA, если используемый протокол AAA способен передать эту информацию.

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.

[1]Foreign Agent.
[2]Mobile Node.

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 Review[1], 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 удалён 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.

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
nmalykh@protokols.ru

[1] Рецензия эксперта.

11. Полное заявление авторских прав

Интеллектуальная собственность

IETF не принимает какой-либо позиции в отношении действительности или объема каких-либо прав интеллектуальной собственности (Intellectual Property Rights или IPR) или иных прав, которые, как может быть заявлено, относятся к реализации или использованию описанной в этом документе технологии, или степени, в которой любая лицензия, по которой права могут или не могут быть доступны, не заявляется также применение каких-либо усилий для определения таких прав. Сведения о процедурах IETF в отношении прав в документах RFC можно найти в BCP 78 и BCP 79.

Копии раскрытия IPR, предоставленные секретариату IETF, и любые гарантии доступности лицензий, а также результаты попыток получить общую лицензию или право на использование таких прав собственности разработчиками или пользователями этой спецификации, можно получить из сетевого репозитория IETF IPR по ссылке http://www.ietf.org/ipr.

IETF предлагает любой заинтересованной стороне обратить внимание на авторские права, патенты или использование патентов, а также иные права собственности, которые могут потребоваться для реализации этого стандарта. Информацию следует направлять в IETF по адресу ietf-ipr@ietf.org.

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.