Internet Engineering Task Force (IETF)
Request for Comments: 8004
Obsoletes: 5204
Category: Standards Track
ISSN: 2070-1721

J. Laganier
Luminate Wireless, Inc.
L. Eggert
NetApp

October 2016

Host Identity Protocol (HIP) Rendezvous Extension

Расширение «встречи» для протокола HIP

Аннотация

Этот документ определяет расширение rendezvous (встреча) для протокола идентификации хостов (Host Identity Protocol или HIP). Расширение rendezvous дополняет HIP и расширение HIP Registration для инициирования взаимодействия между узлами и серверами встречи HIP. Серверы встречи повышают уровень достижимости и работоспособности для мобильных и многоадресных (multihome) узлов HIP. Документ отменяет действие RFC 5204.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc8004.

Оглавление

1. Введение

В документе «The Host Identity Protocol (HIP) Architecture» [HIP-ARCH] вводится механизм встречи (rendezvous), помогающий узлу HIP связаться с часто перемещающимся узлом HIP. Этот механизм включает сторонний (third party) сервер встречи (rendezvous server или RVS), который служит начальной точкой контакта (rendezvous point) для своих клиентов. Клиентами RVS являются узлы HIP, использующие расширение HIP Registration [RFC8003] для регистрации своего сопоставления HIT->IP-адрес на сервере RVS. После регистрации другие узлы HIP могут начать базовый обмен,

[1] Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2] Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

используя IP-адрес RVS вместо текущего IP-адреса искомого узла. По сути, клиенты RVS становятся доступными по IP-адресу RVS. Партнёры могут начать базовый обмен HIP с IP-адресом RVS, который будет транслировать входящие коммуникации для успешного завершения базового обмена.

2. Терминология

В этом разделе определены термины, используемые в данном документе.

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с [RFC2119].

В дополнение к терминам, заданным в спецификации HIP [RFC7401] и HIP Registration Extension [RFC8003] этот документ определяет ещё несколько терминов.

Rendezvous Service - служба встречи
: Служба HIP, обеспечиваемая сервером RVS для встречи с клиентами. RVS обеспечивает ретрансляцию некоторых прибывающих пакетов базового обмена между инициатором и ответчиком.

Rendezvous Server (RVS) - сервер встречи
: Регистратор HIP обеспечивающий сервис встречи.

Rendezvous Client - клиент встречи
: Заявитель HIP, регистрирующийся на RVS для службы встречи.

Rendezvous Registration - регистрация встречи
: Регистрация HIP для службы встречи, организуемая между RVS и клиентом встречи.

3. Обзор работы сервера встречи

На рисунке 1 показан простой базовый обмен HIP без участия сервера RVS. Инициатор начинает обмен с ответчиком напрямую, передавая пакет I1 по IP-адресу ответчика, как указано в спецификации HIP [RFC7401].

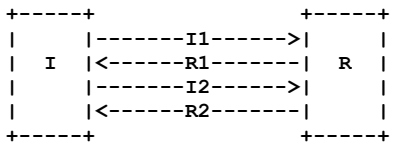


Рисунок 1. Базовый обмен HIP без сервера встречи.

Расширение для мобильных и многодомных конечных хостов (End-Host Mobility and Multihoming) [HIP-HOST-MOB] позволяет узлу HIP уведомить своих партнёров об изменении своего набора адресов IP. Эта спецификация предполагает исходную доступность пары узлов друг для друга.

Однако узел HIP **может** также захотеть своей доступности для будущих партнёров, которые не знают о смене его местоположения. Документ HIP Architecture [HIP-ARCH] вводит серверы RVS, с помощью которых узел HIP **может** зарегистрировать свои теги HIT (Host Identity Tag) и текущие адреса IP. Сервер RVS ретранслирует пакеты HIP, приходящие для этих HIT, по зарегистрированным IP-адресам узла. Когда узел HIP зарегистрирован на RVS, ему **следует** внести IP-адрес своего RVS в свою запись DNS, используя запись ресурса HIP DNS, определённую в расширении HIP DNS [RFC8005].

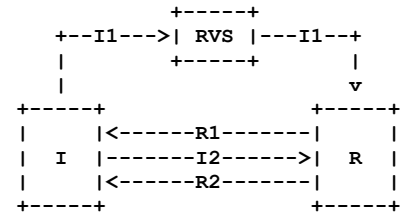


Рисунок 2. Базовый обмен HIP с сервером встречи.

На рисунке 2 показан базовый обмен HIP с участием RVS. Предполагается, что узел HIP R заранее зарегистрировал свои теги HIT и текущие адреса IP на сервере RVS с использованием расширения HIP Registration [RFC8003]. Когда инициатор I пытается организовать контакт с ответчиком R, он должен передать пакет базового обмена I1 по одному из IP-адресов хоста R (если они известны из DNS или иных источников) или одному из серверов RVS хоста R. В примере I получает IP-адрес сервера RVS для хоста R из записи DNS для этого хоста и передаёт пакет базового обмена HIP I1 серверу RVS. Сервер RVS видит, что HIT в полученном пакете I1 не принадлежит ему, и **должен** просмотреть свои текущие регистрации для решения вопроса о ретрансляции пакетов. В примере сервер видит, что HIT относится к хосту R и транслирует пакет I1 по зарегистрированному адресу IP. Хост R после этого завершает базовый обмен без участия RVS, передавая R1 напрямую по IP-адресу хоста I, найденному в пакете I1. В этос спецификации клиент RVS всегда является ответчиком. Однако в некоторых случаях (например, при работе через NAT или межсетевой экран) инициатор может начинать базовый обмен через свой сервер RVS. Спецификация не рассматривает этот вариант, которому следует посвятить отдельный документ.

3.1. Обозначения на рисунках

I, R
: IP-адреса отправителя и получателя в заголовке IP.

HIT-I, HIT-R
: Теги HIT инициатора и ответчика в пакет.

REG_REQ
: Указывает наличие параметра REG_REQUEST в заголовке HIP.

REG_RES
: Указывает наличие параметра REG_RESPONSE в заголовке HIP

FROM:I

Параметр FROM, содержащий IP-адрес I, если он присутствует в заголовке HIP.

RVS_HMAC

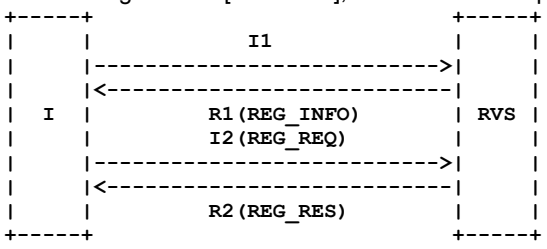
Указывает наличие параметра RVS_HMAC, содержащего хэшированный код аутентификации сообщения (Hashed Message Authentication Code или HMAC) с подходящим ключом регистрации, в заголовке HIP.

VIA:RVS

Указывает наличие параметра VIA_RVS, содержащего IP-адрес сервера встречи RVS, в заголовке HIP.

3.2. Регистрация клиента на сервере встречи

Перед тем, как RVS начнёт ретранслировать пакеты HIP клиенту rendezvous, этот клиент должен зарегистрироваться на RVS с использованием расширения HIP Registration [RFC8003], как показано на рисунке.



Регистрация клиента на сервере встречи.

3.3. Трансляция базового обмена

Если узел HIP и один из его серверов RVS имеют rendezvous-регистрацию, RVS транслируют входящие пакеты I1 (содержащие один из клиентских тегов HIT), переписывая заголовок IP. При этом меняется IP-адрес получателя I1 на один из IP-адресов владельца HIT, т. е. клиента rendezvous. Должна также пересчитываться контрольная сумма IP.

Из-за входной фильтрации на пути от RVS к клиенту [RFC2827] [RFC3013] серверу HIP RVS **следует** заменить IP-адрес отправителя, т. е. I одним из своих адресов IP. Адрес IP для замены **следует** выбирать в соответствии с подходящей спецификацией IPv4 или IPv6 [RFC1122] [RFC6724]. Поскольку замена скрывает IP-адрес инициатора, RVS **должен** добавить в конце параметр FROM, содержащий исходный IP-адрес отправителя пакета. Для параметра FROM **должна** обеспечиваться защита целостности с помощью RVS_HMAC с ключом, соответствующим ключу целостности для регистрации встречи [RFC8003].

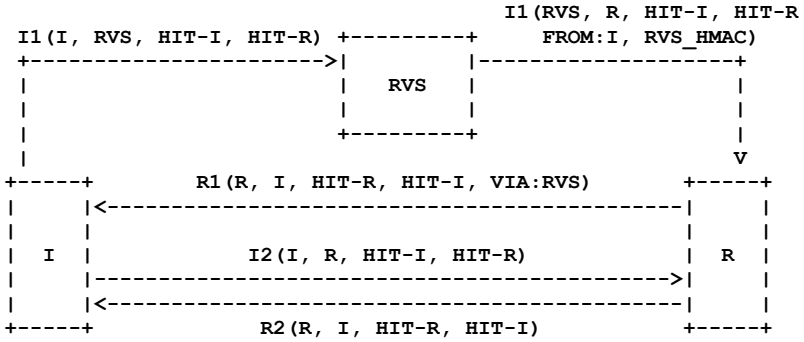


Рисунок 3. Переписывание адреса IP сервером встречи.

Такое изменение пакетов HIP на RVS может вызывать проблемы, поскольку в HIP применяется контроль целостности. I1 не включает параметров HMAC и SIGNATURE, поэтому на сквозную проверку целостности действия RVS не влияют.

Серверу RVS **следует** проверять поле контрольной суммы в пакете I1 до изменения пакета. После изменений контрольная сумма **должна** рассчитываться заново с учётом изменения заголовка HIP, возможного включения параметров FROM и RVS_HMAC, а также псевдозаголовка с обновлёнными IP-адресами отправителя и получателя. Это позволит ответчику проверить контрольную сумму пакета I1 без необходимости анализировать параметры FROM.

4. Расширения сервера встречи

В этом разделе описаны расширения, дополняющие расширение HIP Registration [RFC8003] и позволяющие узлу HIP регистрироваться на RVS для службы встречи (rendezvous service) и уведомлять RVS об изменении своего текущего местоположения. Описано также расширение спецификации HIP [RFC7401], позволяющее организовывать ассоциации HIP через один или несколько серверов HIP RVS.

4.1. Тип регистрации RENDEZVOUS

Эта спецификация добавляет регистрацию в расширение HIP Registration [RFC8003], позволяющую регистрироваться на серверах RVS для «службы встречи» (rendezvous).

Номер	*Тип регистрации*
1	RENDEZVOUS

4.2. Формат и обработка параметров

4.2.1. Параметр RVS_HMAC

Параметр RVS_HMAC является некритическим и отличается от параметра HMAC из спецификации HIP [RFC7401] лишь кодом типа. Это изменение ведёт к тому, что параметр размещается после параметра FROM (в отличие от HMAC)

Type

65500

Length

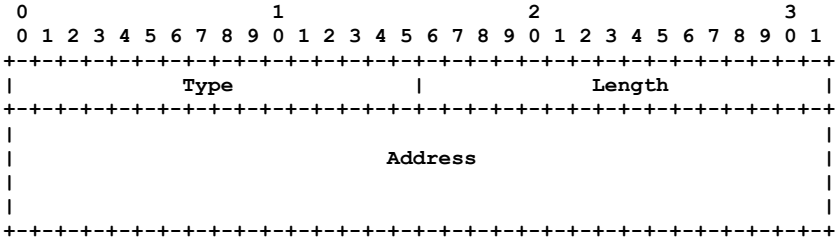
Переменное значение, указывающее размер в октетах без учёта полей Type, Length, Padding.

HMAC

Код HMAC, рассчитанный для пакета HIP без учёта параметра RVS_HMAC и следующих за ним параметров. Для HMAC используется подходящий ключ защиты целостности HIP (HIP-lg или HIP-gl), созданный при регистрации rendezvous. При расчёте HMAC в поле HIP checksum **должно** устанавливаться значение 0, а размер заголовка HIP в базовом заголовке должен рассчитываться без учёта исключаемых параметров. Размером HMAC является размер естественного результата хэш-функции.

Чтобы клиент rendezvous и сервер RVS могли проверить целостность пакетов, передаваемых между ними, **следует** добавлять для защиты пакета параметр RVS_HMAC, рассчитываемый с ключом контроля целостности HIP-lg или HIP-gl, созданным при регистрации. Действительный код RVS_HMAC **следует** включать в каждый пакет, передаваемый между клиентом и сервером, и он **должен** присутствовать при обработке параметра FROM.

4.2.2. Параметр FROM



Type

65498

Length

16

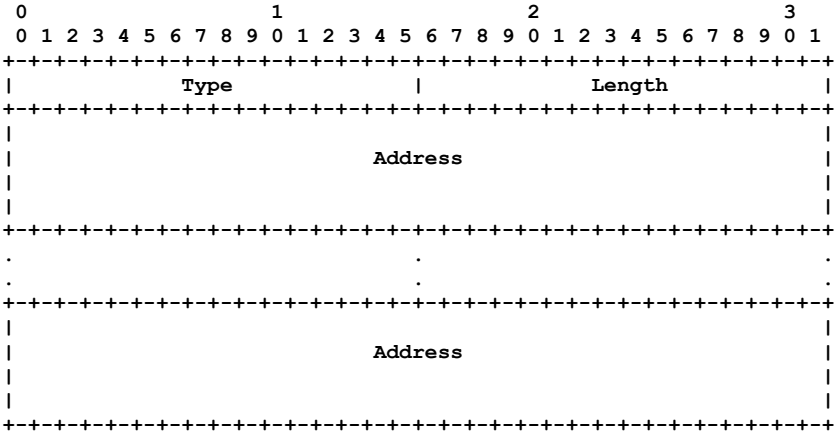
Address

Адрес IPv6 или IPv4 в формате IPv4-in-IPv6.

Сервер RVS **должен** добавлять параметр FROM с исходным IP-адресом отправителя пакета HIP при каждом переписывании IP-адреса отправителя в заголовке IP. Если в пакете уже имеется один или несколько параметров FROM, новый параметр **должен** размещаться сразу после них.

При каждой вставке параметра FROM сервером RVS, он **должен** вставлять параметр RVS_HMAC для защиты целостности пакета (главным образом, адрес IP, включённого в параметр FROM).

4.2.3. Параметр VIA_RVS



Type

65502

Length

Переменное значение.

Address

Адрес IPv6 или IPv4 в формате IPv4-in-IPv6.

После приёма ответчиком ретранслированного пакета I1 он может начать передачу пакетов HIP по IP-адресу инициатора без привлечения сервера RVS. Для целей отладки ответчик **должен** добавлять в конец пакета R1 недавно созданный параметр VIA_RVS, содержащий IP-адрес сервера RVS ретранслировавшего пакет I1. Указание нескольких адресов IP с помощью параметра VIA_RVS выходит за рамки этой спецификации. Основная цель использования параметра VIA_RVS заключается в предоставлении операторам возможности диагностики проблем при создании ассоциаций HIP через сервер RVS.

4.3. Обработка изменённых пакетов

В следующих параграфах описаны отличия в обработке пакетов I1 и R1 при участии RVS в базовом обмене.

4.3.1. Обработка исходящих пакетов I1

Инициатору **не следует** передавать (opportunistic) I1 со значением NULL для HIT получателя по адресу IP, который заведомо принадлежит серверу встречи, если у него нет намерения создать ассоциацию HIP с RVS, не зная его HIT.

Когда RVS переписывает IP-адрес источника пакета I1 из-за выходной фильтрации, он **должен** добавить в I1 параметр FROM с IP-адресом инициатора. Этот параметр FROM **должен** быть учтён в RVS_HMAC с использованием ключа защиты целостности, заданного при регистрации встречи (rendezvous).

4.3.2. Обработка входящих пакетов I1

При получении сервером RVS пакета I1, в котором для адресата указан не его тег HIT, он обращается к своей базе данных для поиска регистрации в службе встречи владельца тега HIT. Если подходящая регистрация найдена, сервер транслирует пакет по зарегистрированному адресу IP. В ином случае пакет отбрасывается.

Серверу RVS **следует** считать входящие пакеты opportunistic I1 (т. е. I1 со значением NULL для HIT получателя) адресованными ему самому и **не следует** пытаться ретранслировать их одному из своих клиентов.

При получении rendezvous-клиентом пакета I1 он **должен** проверить в пакете параметр RVS_HMAC и **следует** отбросить пакет при неудачно проверке. Если проверка RVS_HMAC не прошла, а пакет содержит параметр FROM, этот пакет **должен** отбрасываться.

Клиенту rendezvous, выступающему как ответчик, **следует** отбрасывать пакеты opportunistic I1 с параметром FROM, поскольку этот параметр говорит о том, что пакет I1 был ретранслирован.

4.3.3. Обработка исходящих пакетов R1

Когда ответчик реагирует на пакет I1, транслированный RVS, он **должен** добавить в конец обычного заголовка R1 параметр VIA_RVS с IP-адресам серверов RVS, через которые прошёл пакет.

4.3.4. Обработка входящих пакетов R1

В соответствии со спецификацией HIP [RFC7401] система, получившая пакет R1, **должна** сначала убедиться, что она передавала пакет I1 отправителю R1 (т. е. находится в состоянии I1-SENT). Когда пакет R1 является откликом на ретранслированный пакет I1, эту проверку **следует** выполнять лишь по тегам HIT. Если проверяются и адреса IP, адрес отправителя **должен** сравниваться с IP-адресом из параметра VIA_RVS.

5. Вопросы безопасности

В этом разделе рассматриваются известные угрозы, внесённые описанными расширениями HIP, и их влияние на общую безопасность HIP. В частности, утверждается, что расширения не создают дополнительных угроз для HIP.

Сложно учесть весь спектр угроз, вносимых серверами RVS, поскольку их присутствие проявляется на уровнях IP и HIP. В частности, расширения могут разрешать атаки с перенаправлением, усилением и отражением на уровне IP, а также атаки на сам уровень HIP, например, перехват и изменение сообщений базового обмена HIP (man-in-the-middle).

Если инициатор заранее знает отождествление хоста ответчика при первом контакте с ним через RVS, у него есть возможность проверить подписи в базовом обмене HIP, что позволяет защититься от MiTM-атак (man-in-the-middle). Если инициатор не знает заранее отождествления хоста ответчика (opportunistic Initiator), он практически не способен защитить обмен HIP от таких атак, поскольку нет возможности проверить подлинность при обмене открытыми ключами. Единственным способом снижения угрозы перехвата состояния HIP является требование к ответам R1 на opportunistic I1 содержать тот же IP-адрес отправителя, на который был передан пакет I1. Это сохраняет уровень защиты, присущий современному состоянию Internet.

Однако из соображений простоты эта спецификация не разрешает создавать ассоциации HIP через RVS гибким (opportunistic) способом.

6. Взаимодействие с IANA

В [RFC5204], отменённом этим документом, заданы указанные в таблице определения и резервирование в субреестре Parameter Types реестра Host Identity Protocol (HIP) Parameters.

Значение	*Тип параметра*	*Размер*
65498	FROM	16
65500	RVS_HMAC	переменный
65502	VIA_RVS	переменный

В субреестре Parameter Types реестра Host Identity Protocol (HIP) Parameters ссылки на [RFC5204] заменены ссылками на этот документ.

В [RFC5204], отменённом этим документом, задано приведённое в таблице определение для субреестра Registration Types в реестре Host Identity Protocol (HIP) Parameters.

Значение	*Тип регистрации*
1	RENDEZVOUS

В субреестре Registration Types реестра Host Identity Protocol (HIP) Parameters ссылка на [RFC5204] заменена ссылкой на этот документ.

7. Литература

7.1. Нормативные документы

[RFC1122] Braden, R., Ed., "Requirements for Internet Hosts - Communication Layers", STD 3, RFC 1122, DOI 10.17487/RFC1122, October 1989, <http://www.rfc-editor.org/info/rfc1122>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <http://www.rfc-editor.org/info/rfc6724>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", RFC 7401, DOI 10.17487/RFC7401, April 2015, <http://www.rfc-editor.org/info/rfc7401>.

[RFC8003] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", RFC 8003, DOI 10.17487/RFC8003, October 2016, <http://www.rfc-editor.org/info/rfc8003>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", RFC 8005, DOI 10.17487/RFC8005, October 2016, <http://www.rfc-editor.org/info/rfc8005>.

7.2. Дополнительная литература

[HIP-ARCH] Moskowitz, R. and M. Komu, "Host Identity Protocol Architecture", Work in Progress[1], draft-ietf-hip-rfc4423-bis-14, June 2016.

[HIP-HOST-MOB] Henderson, T., Vogt, C., and J. Arkko, "Host Mobility with the Host Identity Protocol", Work in Progress, draft-ietf-hip-rfc5206-bis-14[2], October 2016.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <http://www.rfc-editor.org/info/rfc2827>.

[RFC3013] Killalea, T., "Recommended Internet Service Provider Security Services and Procedures", BCP 46, RFC 3013, DOI 10.17487/RFC3013, November 2000, <http://www.rfc-editor.org/info/rfc3013>.

[RFC5204] Laganier, J. and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension", RFC 5204, DOI 10.17487/RFC5204, April 2008, <http://www.rfc-editor.org/info/rfc5204>.

Приложение A. Отличия от RFC 5204

Обновлены ссылки HIP с указанием пересмотренных спецификаций HIP.

Благодарности

Перечисленные ниже люди представили содержательные и полезные замечания и/или предложения для улучшения этого документа: Marcus Brunner, Tom Henderson, Miika Komu, Mika Kousa, Pekka Nikander, Juergen Quittek, Justino Santos, Simon Schuetz, Tim Shepard, Kristian Slavov, Martin Stiemerling. Lars Eggert получил финансирование в рамках исследовательской и инновационной программы Европейского союза Horizon 2020 на 2014-2018 годы по гранту № 644866. Этот документ отражает лишь точку зрения авторов и Европейская комиссия не несёт ответственности за какое-либо использование содержащихся в документе сведений.

Спасибо Joel M. Halpern за рецензирование Gen-ART для этого документа в процессе его публикации.

Адреса авторов

Julien Laganier
Luminate Wireless, Inc.
Cupertino, CA
United States of America
Email: julien.ietf@gmail.com

Lars Eggert
NetApp
Sonnenallee 1
Kirchheim 85551
Germany
Phone: +49 151 12055791
Email: lars@netapp.com
URI: http://eggert.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Опубликовано в RFC 9063. *Прим. перев.*
[2]Опубликовано в RFC 8046. *Прим. перев.*