

Internet Engineering Task Force (IETF)
Request for Comments: 6554
Category: Standards Track
ISSN: 2070-1721

J. Hui
JP. Vasseur
Cisco Systems
D. Culler
UC Berkeley
V. Manral
Hewlett Packard Co.
March 2012

An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)

Заголовок IPv6 Routing для заданных отправителем маршрутов с протоколом RPL

Аннотация

В сетях LLN¹ ограничения памяти в маршрутизаторах могут снижать число поддерживаемых ими маршрутов. В некоторых конфигурациях необходимо использовать маршрутизаторы с ограниченной памятью для доставки дейтаграмм узлам сетей LLN. Протокол RPL² может служить в некоторых сетях для хранения большинства (если не всех) маршрутов в одном (например, корень DAG³) или нескольких маршрутизаторах и пересылки дейтаграмм IPv6 с использованием заданного отправителем маршрута для отказа от больших таблиц маршрутизации на устройствах с ограниченной памятью. В этом документе определён новый тип заголовка IPv6 Routing для доставки дейтаграмм в домене маршрутизации RPL.

Статус документа

Этот документ содержит проект стандарта Internet (Internet Standards Track).

Документ является результатом работы IETF⁴ и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG⁵. Дополнительная информация о стандартах Internet доступна в разделе 2 RFC 5741.

Информацию о текущем статусе документа, обнаруженных ошибках и способах обратной связи можно получить, воспользовавшись ссылкой <http://www.rfc-editor.org/info/rfc6554>.

Авторские права

Авторские права ((c) 2012) принадлежат IETF Trust и лицам, указанным в числе авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Simplified BSD License).

Оглавление

1. Введение.....	1
1.1. Уровни требований.....	2
2. Обзор.....	2
3. Формат заголовка RPL Routing.....	3
4. Поведение маршрутизатора RPL.....	4
4.1. Генерация заголовков Source Route.....	4
4.2. Обработка заголовков Source Route.....	4
5. Вопросы безопасности.....	5
5.1. Атаки на заданную отправителем маршрутизацию.....	5
5.2. Атаки ICMPv6.....	6
6. Взаимодействие с IANA.....	6
7. Благодарности.....	6
8. Литература.....	6
8.1. Нормативные документы.....	6
8.2. Дополнительная литература.....	6

1. Введение

RPL является протоколом маршрутизации IPv6 на основе вектора удалённости, предназначенным для сетей LLN [RFC6550]. Ресурсы таких сетей (скорость передачи, производительность процессоров, потребляемая мощность, память) обычно ограничены. В частности, некоторые сети LLN могут использовать маршрутизаторы, где нехватка

¹Low-Power and Lossy Network - сеть со слабым питанием и потерями.

²Routing Protocol for Low-Power and Lossy Networks - протокол маршрутизации для сетей LLN.

³Directed Acyclic Graph - направленный ациклический граф.

⁴Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

⁵Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

памяти позволяет узлам поддерживать лишь небольшое число принятых по умолчанию маршрутов. Однако такие маршрутизаторы с ограниченной памятью приходится использовать для пересылки дейтаграмм и поддержки доступности в LLN.

Для использования путей, включающих маршрутизаторы с ограниченной памятью, в RPL применяется задаваемая источником маршрутизация. В одной из моделей RPL коммутаторы с большими возможностями собирают маршрутные данные и формируют пути к произвольным адресатам в домене RPL. Однако для доставки дейтаграмм требуется механизм заданной отправителем маршрутизации, поддерживаемый IPv6.

В этом документе описан заголовок заданной источником маршрутизации (Source Routing Header или SRH) для использования строго между маршрутизаторами RPL в маршрутном домене RPL, который представляет собой набор маршрутизаторов RPL с общим администрированием. Границы маршрутных доменов определяются системой сетевого управления путём назначения некоторых каналов внешними (междоменными).

1.1. Уровни требований

Ключевые слова **необходимо** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не нужно** (SHALL NOT), **следует** (SHOULD), **не следует** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

2. Обзор

Формат SRH основан на формате заголовка маршрутизации типа 0 (RH0) [RFC2460]. Однако SRH добавляет механизм сжатия записей source route при использовании всеми записями одного префикса с передачей адреса получателя IPv6 в пакете с опцией SRH - этот типовой вариант работы в LLN с заданной отправителем маршрутизацией. Механизм сжатия снижает расход дефицитных ресурсов, таких как пропускная способность канала.

SRH отличается от RH0 также правилами обработки для смягчения проблем безопасности, которые привели к отказу от RH0 [RFC5095]. Во-первых, маршрутизаторы RPL реализуют строгую политику маршрутизации от источника, где каждый узел пересылки IPv6 между отправителем и получателем указывается в SRH. Отметим, что source route может быть подмножеством пути между фактическим отправителем и получателем, как описано ниже. Во-вторых, SRH применяется лишь между маршрутизаторами RPL в одном домене маршрутизации RPL. Граничные маршрутизаторы RPL, отвечающие за соединение доменов маршрутизации RPL и доменов IP с другими протоколами маршрутизации, не пропускают дейтаграммы с заголовком SRH через границу домена маршрутизации RPL. В-третьих, маршрутизатор RPL для предотвращения петель отбрасывает дейтаграммы, включающие несколько адресов, назначенных интерфейсам данного маршрутизатора.

Имеется 2 случая, определяющие способ включения SRH, когда маршрутизатору RPL нужен заголовок SRH для доставки дейтаграмм адресату.

1. Если SRH задаёт полный путь от источника к получателю, маршрутизатор помещает SRH непосредственно в дейтаграмму.
2. Если SRH задаёт лишь часть пути от источника к адресату, маршрутизатор использует туннель IPv6-in-IPv6 [RFC2473] и помещает SRH во внешний заголовок IPv6. Использование туннеля гарантирует неизменность дейтаграммы при доставке и отправку сообщений ICMP об ошибках источнику заголовка SRH, а не исходной дейтаграммы.

В сети RPL вариант 1 возникает при размещении источника и получателя в одном маршрутном домене RPL и применяется один заголовок SRH для задания всего пути от источника к получателю, как показано на рисунке 1.

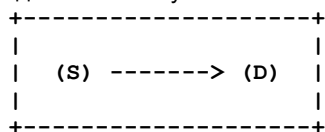


Рисунок 1. Домен маршрутизации RPL.

В этом примере дейтаграммы от источника S к адресату D имеет вид, показанный на рисунке 2.

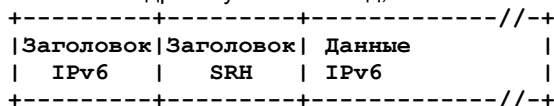


Рисунок 2. Структура пакета.

Адрес S передаётся в поле Source Address заголовка IPv6, адрес D - в последней записи SRH на всех интервалах пересылки, кроме последнего, где он переносится в поле Destination Address заголовка IPv6 в пакете с SRH.

Вариант 2 возникает в сети RPL для всех дейтаграмм, отправитель и/или получатель которых находится за пределами домена маршрутизации RPL, как показано на рисунке 3.



Рисунок 3. Взаимодействие с внешним доменом.

На рисунке 3 R указывает граничный маршрутизатор RPL (соединение с другими доменами маршрутизации) или обычный маршрутизатор RPL (подключение хоста). Структура дейтаграммы в домене маршрутизации RPL показана на рисунке 4.

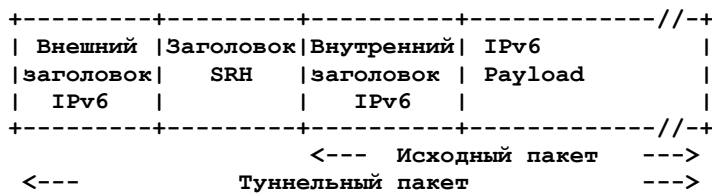


Рисунок 4. Структура дейтаграммы в RPL.

Отметим, что внешний заголовок (с SRH) добавляют и удаляют маршрутизаторы RPL.

Вариант 2 возникает также в случае, когда маршрутизатору RPL нужно вставить заданный источником маршрут при пересылке дейтаграммы. Один из таких вариантов использования в сети RPL возникает, когда весь поток трафика RPL идёт через граничный маршрутизатор и тот использует заданные источником маршруты для доставки дейтаграмм адресатам. При включении SRH с использованием туннеля граничный маршрутизатор инкапсулирует полученную дейтаграмму в исходной форме с использованием IPv6-in-IPv6 и включает SRH во внешний заголовок IPv6.

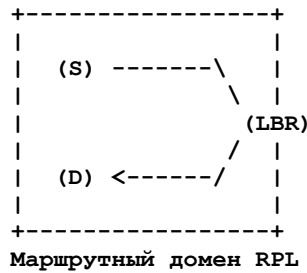
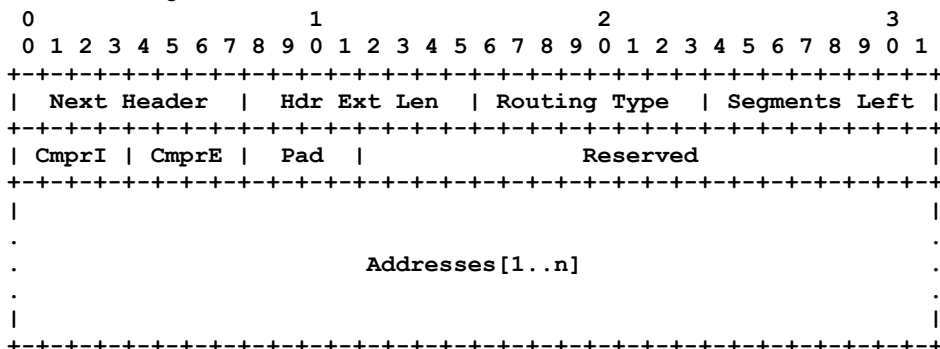


Рисунок 5. Граничный маршрутизатор.

В примере на рисунке 5 дейтаграммы от S к D проходят через граничный маршрутизатор сети LLN (LBR). Между S и LBR дейтаграммы маршрутизируются с использованием графа DAG, построенного RPL и не включают SRH. Маршрутизатор LBR инкапсулирует полученные дейтаграммы с использованием IPv6-in-IPv6 и SRH во внешнем заголовке IPv6.

3. Формат заголовка RPL Routing

Формат заголовка Source Routing Header показан ниже.



Next Header

8-битовый селектор, указывающий тип заголовка сразу после заголовка Routing. Применяются те же значения, что и в поле IPv6 Next Header [RFC2460].

Hdr Ext Len

8-битовое целое число без знака, указывающее размер заголовка Routing в 8-октетных словах без учёта первых 8 октетов. Отметим, что при сжатии Addresses[1..n] (Cmprl или CmprE отлично от 0) значение Hdr Ext Len не равно удвоенному числу адресов.

Routing Type

8-битовый селектор, указывающий вариант заголовка Routing. Для SRH нужно устанавливать Routing Type = 3.

Segments Left

8-битовое целое число без знака, указывающее количество оставшихся сегментов маршрута, т. е. явно заданных промежуточных узлов, которые нужно пройти до попадания к адресату. Источник SRH устанавливает в этом поле значение n, равное числу адресов в Addresses[1..n].

Cmprl

4-битовое целое число без знака, указывающее количество опущенных октетов префикса для каждого сегмента, кроме последнего (т. е. сегментов 1 - n-1). Например, SRH с полными адресами IPv6 в Addresses[1..n-1] устанавливает Cmprl = 0.

CmprE

4-битовое целое число без знака, указывающее количество опущенных октетов префикса для последнего сегмента (т. е. сегмента n). Например, SRH с полными адресами IPv6 в Addresses[1..n-1] устанавливает CmprE = 0.

Pad

4-битовое целое число без знака, указывающее количество октетов, используемых для заполнения после Address[n] в конце SRH.

Reserved

Резервное поле, которое **должно** устанавливаться в 0 при передаче, а получатель **должен** игнорировать его.

Address[1..n]

Вектор адресов с номерами 1 - n. Каждый элемент [1..n-1] имеет размер (16 - Cmprl), а элемент [n] - (16-CmprE).

Создатель SRH помещает адрес IPv6 следующего (первого) узла пересылки в поле Destination Address заголовка IPv6, а адрес IPv6 второго интервала пересылки в первый элемент Address[1..n] (т. е. Address[1]).

SRH использует такой же базовый формат как заголовок 0 типа 0 [RFC2460]. При передаче полных адресов IPv6 поля Cmprl, CmprE, Pad имеют значение 0 и единственным различием между SRH и Type 0 является кодирование поля Routing Type.

В базовой конфигурации маршрутного домена RPL все маршрутизаторы домена используют общий префикс. Поля Cmprl, CmprE и Pad позволяют сжать вектор Address[1..n] при использовании одного префикса во всех записях, совпадающего с префиксом поля IPv6 Destination Address в заголовке пакета с SRH. Поля Cmprl и CmprE указывают число октетов префикса, совпадающих с IPv6 Destination Address в пакете с SRH. Общие октеты не передаются в заголовке Routing и каждая запись Address[1..n-1] имеет размер (16 - Cmprl), а Address[n] - (16 - CmprE) октетов. При отличном от 0 Cmprl или CmprE между последней записью Address[n] и концом заголовка Routing могут остаться неиспользуемые октеты. Поле Pad указывает число таких октетов, для которых применяется заполнение. Если оба поля Cmprl и CmprE имеют значение 0, поле Pad **должно** содержать 0.

В SRH **недопустимо** задавать путь, проходящий через узел более 1 раза. При создании SRH источник может не знать сопоставления адресов IPv6 с узлами. Источник **должен** по меньшей мере исключить неоднократное включение в заголовок адресов IPv6 и отсутствие в SRH адресов отправителя и получателя инкапсулирующей дейтаграммы.

Групповые адреса **недопустимо** указывать в SRH или поле IPv6 Destination Address дейтаграммы с SRH.

4. Поведение маршрутизатора RPL

4.1. Генерация заголовков Source Route

Для доставки дейтаграммы IPv6 адресату маршрутизатору может потребоваться создать новый заголовок SRH и строго задать source route. Когда маршрутизатор является источником исходного пакета и известно, что адресат находится в том же маршрутном домене RPL, маршрутизатору **следует** включать SRH напрямую в исходный пакет. В иных случаях маршрутизатор **должен** использовать туннель IPv6-in-IPv6 [RFC2473] и помещать SRH в заголовок туннеля. Использование туннеля IPv6-in-IPv6 обеспечивает неизменность доставляемой дейтаграммы и доставку сообщений ICMPv6 об ошибках, связанных с SRH, создавшему заголовок SRH маршрутизатору.

При использовании туннеля IPv6-in-IPv6 для соблюдения IPv6 Hop Limit в исходной дейтаграмме маршрутизатор RPL, создающий SRH **должен** установить Segments Left меньше значения IPv6 Hop Limit в исходной дейтаграмме при пересылке. Если source route длиннее чем IPv6 Hop Limit в исходной дейтаграмме, в SRH следует включать лишь начальные узлы пересылки (определяется IPv6 Hop Limit в исходной дейтаграмме). Если маршрутизатор RPL не является источником исходной дейтаграммы, значение поля IPv6 Hop Limit в ней уменьшается до создания SRH. После генерации SRH маршрутизатор RPL уменьшает IPv6 Hop Limit исходной дейтаграммы на SRH Segments Left. Обработка SRH Segments Left и IPv6 Hop Limit исходной дейтаграммы обеспечивает возникновение ошибок ICMPv6 Time Exceeded как в обычных сетях IPv6 без туннелирования дейтаграмм.

Для предотвращения фрагментации желательнее использовать MTU, позволяющие дополнительно расширить заголовок по меньшей мере до 1280 + 40 (внешний заголовок IP) + SRH_MAX_SIZE, где SRH_MAX_SIZE - максимальная длина пути в данной сети RPL. Однако для этого взаимодействующие конечные точки должны знать MTU на пути (например, от Path MTU Discovery). К сожалению большие значения MTU могут быть недоступны на некоторых каналах (например, 1280 октетов для каналов 6LoWPAN¹). Однако предполагается, что большая часть трафика в сетях этого типа состоит из пакетов размером меньше MTU и фрагментация не вызовет проблем.

4.2. Обработка заголовков Source Route

Как указано в [RFC2460], заголовок маршрутизации не рассматривается и не обрабатывается, пока пакет не достигнет узла, указанного в поле Destination Address заголовка IPv6, где диспетчеризация по полю Next Header непосредственно предшествующего заголовка приводит к вызову модуля заголовка Routing.

¹IPv6 Low-Power Wireless Personal Area Network - персональная беспроводная сеть IPv6 со слабым питанием.

Назначение SRH очень похоже на функции заголовка Routing типа 0, определённого в [RFC2460]. После обработки заголовка маршрутизации и представления дейтаграммы IPv6 модулю IPv6 для дальнейшей обработки поле IPv6 Destination Address содержит адрес следующего узла пересылки. Если пересылаемая дейтаграмма IPv6 содержит заголовок SRH с отличным от 0 полем Segments Left и IPv6 Destination Address не относится к тому же каналу, маршрутизатор **должен** отбросить дейтаграмму и ему **следует** передать сообщение ICMP Destination Unreachable (ICMPv6 Type 1) с ICMPv6 Code = 7 по адресу отправителя в пакете. Этот код ICMPv6 указывает, что IPv6 Destination Address не относится к тому же каналу и маршрутизатор не может выполнить требование строгой маршрутизации, заданной источником. При генерации сообщения ICMPv6 об ошибке **должны** соблюдаться правила параграфа 2.4 в [RFC4443].

Для обнаружения петель в SRH маршрутизатор **должен** проверить наличие в заголовке нескольких адресов своих интерфейсов. Если какой-либо адрес указан более 1 раза с разделением по меньшей мере одним адресом другого маршрутизатора, пакет **должен** отбрасываться и маршрутизатору **следует** передать сообщение ICMP Parameter Problem с кодом 0 по адресу отправителя. Хотя такая проверка существенно увеличивает издержки при обработке пакетов, она нужна для смягчения поглощающих пропускную способность атак, которые привели в своё время к отказу от заголовка RH0 [RFC5095].

Ниже приведён псевдо-код алгоритма обработки SRH.

```

if Segments Left = 0 {
    обрабатывается следующий заголовок в пакете, тип которого
    указывает поле Next Header в заголовке Routing
}
else {
    рассчитывается число адресов в заголовке Routing
    n = (((Hdr Ext Len * 8) - Pad - (16 - CmprE)) / (16 - CmprI)) + 1

    if Segments Left > n {
        передаётся сообщение ICMP Parameter Problem с Code = 0, по Source
        Address с указанием Segments Left и пакет отбрасывается
    }
    else {
        Segments Left уменьшается на 1

        рассчитывается индекс следующего адреса (i) в векторе адресов как
        n - Segments Left

        if Address[i] или IPv6 Destination Address является групповым {
            пакет отбрасывается
        }
        else if 2 или более записи в Address[1..n] относятся к локальному
        интерфейсу и разделены хотя бы 1 адресом, не назначенным
        локальному интерфейсу {
            передаётся ICMP Parameter Problem (Code 0) и пакет отбрасывается
        }
        else {
            меняются местами IPv6 Destination Address и Address[i]

            if IPv6 Hop Limit ≤ 1 {
                передаётся ICMP Time Exceeded, Hop Limit Exceeded в сообщении
                Transit по Source Address и пакет отбрасывается
            }
            else {
                Hop Limit уменьшается на 1

                пакет заново представляется модулю IPv6 для передачи новому
                получателю
            }
        }
    }
}
}

```

Маршрутизаторы RPL отвечают за вставку SRH лишь при передаче между собой.

1. Для дейтаграмм, адресованных маршрутизатору RPL, он выполняет обработку обычным способом. Например, при включении SRH с использованием туннеля, для которого маршрутизатор служит конечной точкой, он удаляет внешний заголовок IPv6 вместе с SRH.
2. Дейтаграммы, адресованные другим узлам домена маршрутизации RPL, пересылаются в нужный интерфейс.
3. Дейтаграммы для узлов за пределами маршрутного домена RPL отбрасываются, если внешний заголовок IPv6 содержит заголовок SRH, созданный не маршрутизатором RPL, который пересылает дейтаграмму.

5. Вопросы безопасности

5.1. Атаки на заданную отправителем маршрутизацию

Механизмы защиты сообщений RPL, определённые в [RFC6550], не применимы к заголовкам RPL SRH. Данная спецификация не обеспечивает механизмов защиты целостности, конфиденциальности и аутентификации SRH.

В [RFC5095] заголовок Routing типа 0 был отменен из-за возможности атак, указанных в этом документе. Такие атаки включают обход устройств фильтрации, доступ в недостижимые иными путями системы Internet, раскрытие топологии сетей, истощение пропускной способности и нарушение anycast-адресации.

Поскольку в этом документе указано, что заголовок SRH используется лишь в домене маршрутизации RPL, указанные атаки невозможно организовать извне. Как указано в этом документе, маршрутизаторы RPL **должны** отбрасывать на границе домена RPL входящие и исходящие дейтаграммы с SRH в заголовках расширения IPv6.

Однако такие атаки могут быть организованы из домена маршрутизации RPL. Для ослабления атак на истощение пропускной способности данная спецификация требует от маршрутизаторов RPL проверять наличие петель в SRH и отбрасывать дейтаграммы с петлями. Атаки с обходом фильтров и доступом в закрытые системы Internet не так актуальны в mesh-сетях, поскольку их топология очень динамична. Протокол маршрутизации RPL разработан для обеспечения доступности всех устройств в домене маршрутизации RPL и может использовать маршруты, проходящие любое число устройств в произвольном порядке.

Атаки указанных типов и другие (например, нарушение anycast-адресации и раскрытие топологии сети) возможны в домене RPL при использовании этой спецификации.

5.2. Атаки ICMPv6

Создание сообщений ICMPv6 об ошибках может использоваться для организации атак на службы путём отправки вызывающих ошибки SRH в последовательных дейтаграммах. Реализация, корректно следующая параграфу 2.4 в [RFC4443], будет защищена механизмом ограничения частоты ICMPv6.

6. Взаимодействие с IANA

В этом документе определён новый тип заголовка IPv6 Routing «RPL Source Route Header», которому агентство IANA выделило значение 3. Документ определяет также новый код ICMPv6 Destination Unreachable «Error in Source Routing Header», для которого агентство IANA выделило значение 7.

7. Благодарности

Авторы благодарны Jari Arkko, Ralph Droms, Adrian Farrel, Stephen Farrell, Richard Kelsey, Suresh Krishnan, Erik Nordmark, Pascal Thubert, Sean Turner и Tim Winter за комментарии и предложения, которые помогли создать документ.

8. Литература

8.1. Нормативные документы

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#)¹, December 1998.

[RFC2473] Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", [RFC 4443](#), March 2006.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

8.2. Дополнительная литература

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", [RFC 6550](#), March 2012.

Адреса авторов

Jonathan W. Hui

Cisco Systems

170 West Tasman Drive

San Jose, California 95134

USA

Phone: +408 424 1547

E-Mail: jonhui@cisco.com

JP. Vasseur

Cisco Systems

11, Rue Camille Desmoulins

Issy Les Moulineaux 92782

France

E-Mail: jpv@cisco.com

¹Заменен [RFC 8200](#). Прим. перев.

David E. Culler

UC Berkeley
465 Soda Hall
Berkeley, California 94720
USA
Phone: +510 643 7572
EMail: culler@cs.berkeley.edu

Vishwas Manral

Hewlett Packard Co.
19111 Pruneridge Ave.
Cupertino, California 95014
USA
EMail: vishwas.manral@hp.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru