

## The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams

### Аннотация

Протокол RPL<sup>1</sup> включает маршрутные сведения в дейтаграммах плоскости данных для быстрого обнаружения несогласованностей в топологии маршрутов. В этом документе описана опция RPL, передаваемая между маршрутизаторами RPL для обмена такой информацией.

### Статус документа

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

Документ является результатом работы IETF<sup>2</sup> и представляет собой согласованное мнение сообщества IETF. Документ был вынесен на публичное рассмотрение и одобрен для публикации IESG<sup>3</sup>. 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/rfc6553>.

### Авторские права

Авторские права ((с) 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 опции RPL.....	2
4. Поведение маршрутизатора RPL.....	2
5. Вопросы безопасности.....	3
5.1. Атаки на согласованность DAG.....	3
5.2. Атаки на согласованность DAO.....	3
6. Взаимодействие с IANA.....	3
7. Благодарности.....	4
8. Литература.....	4
8.1. Нормативные документы.....	4
8.2. Дополнительная литература.....	4

## 1. Введение

RPL представляет собой протокол маршрутизации IPv6 на основе векторов удалённости, разработанный для сетей LLN<sup>4</sup> [RFC6550]. Такие сети обычно имеют ограничения по питанию и/или производительности каналов. Для экономии дефицитных ресурсов протокол должен экономно генерировать управляющий трафик. Однако это противоречит потребности в быстром распространении маршрутов для своевременного устранения несогласованностей в них.

Для минимизации расхода ресурсов в RPL применяется медленный проактивный процесс построения и поддержки маршрутной топологии вкупе с реактивным и динамичным процессом устранения несогласованности маршрутов. В установившемся состоянии RPL поддерживает топологию маршрутов с помощью низкоскоростной передачи специальных сигналов (beacon - маячок). Однако при обнаружении несогласованности, которая может препятствовать доставке дейтаграмм, RPL временно повышает скорость передачи сигналов для быстрого устранения несогласованности. Эта операция динамического управления скоростью контролируется динамическими таймерами (Trickle), определёнными в [RFC6206]. В отличие от других протоколов маршрутизации (например, OSPF [RFC2328]), RPL обнаруживает несогласованности за счёт проверки путей данных путём включения маршрутных данных в передаваемые дейтаграммы. Благодаря этому, механизмы восстановления включаются лишь при необходимости, позволяя плоскостям управления и данных работать в близком масштабе времени. Основным мотивом проверки путей данных в LLN служит аккуратная привязка управляющего трафика к трафику данных. Интуитивно понятно, что не требуется решать проблемы маршрутизации (они могут быть временными) при отсутствии трафика данных.

<sup>1</sup>Routing Protocol for Low-Power and Lossy Networks - протокол маршрутизации для сетей LLN.

<sup>2</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

<sup>3</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

<sup>4</sup>Low-Power and Lossy Networks - сети со слабым питанием и потерями.

RPL создаёт направленный ациклический граф (Directed Acyclic Graph или DAG), который пытается минимизировать стоимость пути к корню DAG на основании набора параметров метрики и предметных функций (Objective Function или OF). В некоторых случаях могут возникать петли и в RPL применяется метод обнаружения петель в пути данных. Это одно из требований RPL и в будущем может быть задано другое использование пути данных.

Для решения задачи в этом документе определена новая опция IPv6 (RPL Option), передаваемая в заголовке IPv6 Hop-by-Hop. Опция RPL передаётся лишь между маршрутизаторами RPL, участвующими в одном экземпляре RPL Instance.

## 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

Опция RPL обеспечивает механизм включения маршрутных данных в каждую дейтаграмму, пересылаемую маршрутизатором. При получении дейтаграммы с маршрутными данными маршрутизаторы RPL обрабатывают эти данные для поддержки топологии маршрутов.

Каждый маршрутизатор RPL на пути доставки пакета обрабатывает и обновляет RPL Option. Если в принятом пакете опции RPL ещё нет, маршрутизатор RPL должен вставить RPL Option в заголовок до пересылки пакета другому маршрутизатору RPL. Этот документ задаёт также применение туннелей IPv6-in-IPv6 [RFC2473] при добавлении в пакет опции RPL, гарантирующее неизменность исходного пакета и возврат сообщений ICMP при возникновении ошибки источнику опции RPL, а не отправителю исходного пакета.

## 3. Формат опции RPL

RPL Option передаётся в заголовке IPv6 Hop-by-Hop Options, следующем сразу после заголовка IPv6, и выравнивается по границе 2n. Формат опции показан на рисунке 1.

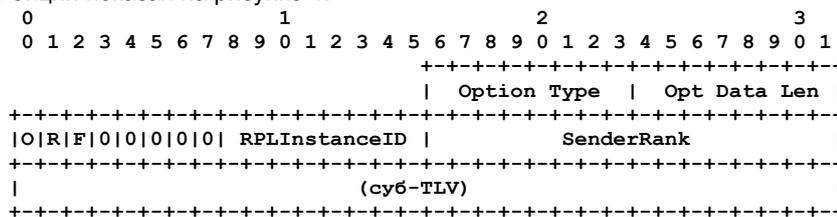


Рисунок 1. RPL Option.

### Option Type

0x63

### Opt Data Len

8-битовое поле указывающее размер опции в октетах без учёта полей Option Type и Opt Data Len.

### O (Down)

Флаг, определённый в параграфе 11.2 [RFC6550], который **нужно** обрабатывать в соответствии с указанным параграфом в [RFC6550].

### R (Rank-Error)

Флаг, определённый в параграфе 11.2 [RFC6550], который **нужно** обрабатывать в соответствии с указанным параграфом в [RFC6550].

### F (Forwarding-Error)

Флаг, определённый в параграфе 11.2 [RFC6550], который **нужно** обрабатывать в соответствии с указанным параграфом в [RFC6550].

### RPLInstanceID

8-битовое поле, определённое в параграфе 11.2 [RFC6550], которое **нужно** обрабатывать в соответствии с указанным параграфом в [RFC6550].

### SenderRank

16-битовое поле, определённое в параграфе 11.2 [RFC6550], которое **нужно** обрабатывать в соответствии с указанным параграфом в [RFC6550].

Два старших бита поля Option Type **должны** иметь значения 01, а третий - 1. На основании этих битов в соответствии с [RFC2460] узлы, не понимающие опцию, **должны** отбрасывать пакет. В соответствии с [RFC2460] значения опции RPL Option предполагаются изменяющимися в пути. Размер данных RPL Option является переменным.

Действия, выполняемые при использовании RPL Option, и возможный набор TLV внутри опции RPL, **должны** задаваться в RFC для использующего опцию протокола. Этот документ не определяет TLV. Устройство RPL **должно** пропускать непонятные TLV и пытаться обработать последующие TLV.

## 4. Поведение маршрутизатора RPL

Дейтаграммы, передаваемые между маршрутизаторами RPL, **должны** включать RPL Option или RPL Source Route Header ([RFC6554]) и **могут** включать то и другое. В дейтаграммы с заголовком Source Routing (SRH) не обязательно включать RPL Option, поскольку источник и промежуточные маршрутизаторы обеспечивают отсутствие петель в SRH.

Когда маршрутизатор является источником исходного пакета, а получатель заведомо относится к тому же экземпляру RPL, маршрутизатору **следует** включать RPL Option непосредственно в исходный пакет. В иных случаях маршрутизаторы **должны** использовать туннели IPv6-in-IPv6 [RFC2473] и помещать RPL Option в заголовок туннеля. Использование туннеля IPv6-in-IPv6 обеспечивает неизменность исходной дейтаграммы в пути и доставку сообщений ICMPv6 при ошибках, связанных с RPL Option, маршрутизатору, создавшему эту опцию.

Маршрутизатор RPL выбирает следующий маршрутизатор RPL, которому следует обрабатывать исходный пакет в качестве точки выхода из туннеля. В некоторых случаях выходом из туннеля является последний маршрутизатор RPL

на пути к адресату исходного пакета и пакет проходит лишь через один туннель. Примером может служить случай, когда конечный получатель или маршрутизатор, к которому он подключён относится к тому же экземпляру RPL<sup>1</sup>.

В иных случаях точкой выхода из туннеля не является последний маршрутизатор RPL на пути и исходный пакет может проходить через несколько туннелей. Примером может служить случай, когда маршрутизатор RPL просто пересылает пакет одному из родителей DODAG<sup>2</sup>, где маршрутизатор RPL устанавливает точку выхода из туннеля. При поэтапной пересылке исходного пакета маршрутизатор RPL лишь определяет следующий интервал пересылки к адресату.

Маршрутизатор RPL, получивший адресованный ему пакет IPv6-in-IPv6, обрабатывает туннельный пакет в соответствии и разделом 3 в [RFC2473]. Перед декапсуляцией IPv6 маршрутизатор RPL **должен** обработать опцию RPL, если она имеется. Если после декапсуляции IPv6 маршрутизатор определит, что следует переслать исходный пакет другому маршрутизатору RPL, он **должен** снова инкапсулировать пакет в туннель IPv6-in-IPv6 для включения RPL Option. Поля в опции RPL, которые не меняются на этапах пересылки, **должны** совпадать с полученными из предыдущего туннеля.

Маршрутизаторы RPL отвечают за использование RPL Option только между собой.

1. Адресованные маршрутизатору RPL дейтаграммы тот обрабатывает обычным способом. Например, при включении RPL Option с использованием туннеля, конечной точкой которого является маршрутизатор RPL, этот маршрутизатор удаляет внешний заголовок IPv6, одновременно удаляя и RPL Option.
2. Дейтаграммы, адресованные в другие точки того же экземпляра RPL, пересылаются в нужный интерфейс.
3. Дейтаграммы, адресованные узлам за пределами RPL Instance, отбрасываются, если их внешний заголовок IPv6 содержит опцию RPL, не созданную переславшим дейтаграмму маршрутизатором RPL.

Для предотвращения фрагментации желательно применять значения MTU, допускающие расширение заголовка, например, не меньше 1280 + 40 (внешний заголовок IP) + RPL\_OPTION\_MAX\_SIZE, где RPL\_OPTION\_MAX\_SIZE - максимальный размер заголовка RPL Option для 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 доступны не на всех каналах (например, на каналах 6LoWPAN<sup>3</sup> MTU = 1280 октетов). Однако предполагается, что большая часть трафика в таких сетях передаётся в пакетах размером меньше MTU, поэтому снижение производительности из-за фрагментации не будет значительным.

## 5. Вопросы безопасности

Опция RPL помогает маршрутизаторам RPL обнаруживать несогласованность маршрутизации. Механизмы защиты сообщений RPL, заданные в [RFC6550], не применяются для RPL Option.

### 5.1. Атаки на согласованность DAG

Используя флаг O и поле SenderRank, атакующий может убедить маршрутизаторы RPL в наличии несогласованности DAG внутри экземпляра RPL, указанного в поле RPLInstanceID. Это заставит маршрутизатор RPL сбросить таймер DIO<sup>4</sup> Trickle и начать более частую передачу сообщений DIO.

Для предотвращения неприемлемого влияния на работу сети реализация **может** ограничить частоту сброса таймера Trickle при получении RPL Option значением MAX\_RPL\_OPTION\_RANK\_ERRORS в течение часа. В качестве значения MAX\_RPL\_OPTION\_RANK\_ERRORS **рекомендуется** 20.

### 5.2. Атаки на согласованность DAO

В режиме Storing маршрутизаторы RPL поддерживают состояние нисходящей (Downward) маршрутизации. При нормальной работе опция RPL помогает маршрутизаторам RPL очищать устаревшее состояние нисходящей маршрутизации, используя флаг F для указания невозможности доставки дейтаграммы потомком и необходимости её передачи через другого потомка. С помощью этого флага атакующий может вынудить маршрутизатор RPL сбросить состояние маршрутизации Downward.

Для предотвращения неприемлемого влияния на работу сети реализация **может** ограничить частоту отбрасывания состояний маршрутизации Downward при получении RPL Option значением MAX\_RPL\_OPTION\_FORWARD\_ERRORS в течение часа. В качестве значения MAX\_RPL\_OPTION\_FORWARD\_ERRORS **рекомендуется** 20.

В режиме Non-Storing состояние Downward поддерживают лишь граничные маршрутизаторы LBR<sup>5</sup>. Поскольку маршрутизаторы RPL не поддерживают состояние нисходящей маршрутизации, опцию RPL в этом режиме невозможно использовать для организации атак.

## 6. Взаимодействие с IANA

Агентство IANA выделило новое значение в реестре Destination Options and Hop-by-Hop Options, как показано в таблице.

Шестнадцатеричное значение	Двоичное значение			Описание	Документ
0x63	act	chg	rest	RPL Option	[RFC6553]
	01	1	00011		

Как сказано в [RFC2460], первые 2 бита указывают, что узел IPv6 **должен** отбрасывать пакет с неизвестным типом опции, а третий говорит, что данные опции могут меняться на маршруте. Остальные биты задают тип опции.

Агентство IANA создало реестр RPL-option-TLV для TLV, передаваемых в заголовке RPL Option, с выделением новых кодов по процедуре IETF Review [RFC5226]. Поле типа имеет размер 8 битов и может содержать значения от 0 до 255.

<sup>1</sup>Экземпляру RPL, к которому относится отправитель исходного пакета. *Прим. перев.*

<sup>2</sup>Destination-Oriented DAG - ориентированный на адресата направленный ациклический граф (DAG).

<sup>3</sup>IPv6 Low-Power Wireless Personal Area Network - персональная беспроводная сеть IPv6 со слабым питанием.

<sup>4</sup>DODAG Information Object - объект информации DODAG.

<sup>5</sup>Low-Power and Lossy Network Border Router - граничный маршрутизатор сети LLN.

## 7. Благодарности

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

[RFC2328] Moy, J., "OSPF Version 2", STD 54, [RFC 2328](#), April 1998.

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

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

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, [RFC 5226](#), May 2008.

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko, "The Trickle Algorithm", RFC 6206, March 2011.

[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.

### 8.2. Дополнительная литература

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", [RFC 6554](#), 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](mailto:jonhui@cisco.com)

##### JP. Vasseur

Cisco Systems

11, Rue Camille Desmoulins

Issy Les Moulineaux 92782

France

E-Mail: [jpv@cisco.com](mailto:jpv@cisco.com)

#### Перевод на русский язык

Николай Малых

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)