

## Возможность выходной фильтрации маршрутов для BGP-4

### Outbound Route Filtering Capability for BGP-4

#### Статус документа

В этом документе содержится проект стандарта протокола Internet для сообщества Internet и приглашение к дискуссии в целях развития и совершенствования. Текущее состояние стандартизации протокола и его статус можно узнать из документа Internet Official Protocol Standards (STD 1). Документ может распространяться свободно.

#### Аннотация

В этом документе определён основанный на протоколе BGP механизм, позволяющий узлу BGP передавать своим партнёрам набор фильтров ORF<sup>1</sup>, которые этот партнёр будет использовать для ограничения/фильтрации исходящих маршрутных обновлений для данного узла.

#### 1. Введение

В настоящее время обычной практикой для узлов BGP [BGP-4] является приём маршрутных обновлений от партнёра с последующей фильтрацией нежелательных обновлений на основе локальной политики маршрутизации. Поскольку генерация и передача маршрутных обновлений отправителем, равно как их обработка получателем, потребляют ресурсы, отказ от генерации нежелательных маршрутных обновлений может давать преимущества.

В этом документе определён основанный на протоколе BGP механизм, позволяющий узлу BGP передать своему партнёру BGP набор фильтров ORF. Партнёр будет применять полученные фильтры в дополнение к фильтрам, заданным в его локальной конфигурации (если таковые имеются), для ограничения/фильтрации маршрутных обновлений, передаваемых данному узлу.

#### 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 интерпретируются в соответствии с RFC 2119 [RFC2119].

#### 3. Фильтр ORF

В контексте этого документа термины «идентификатор семейства адресов» (AFI<sup>2</sup>) и «дополнительный идентификатор семейства адресов» (SAFI<sup>3</sup>) трактуются в соответствии с [BGP-MP].

Концептуально элемент ORF представляет собой последовательность полей <AFI/SAFI, ORF-Type<sup>4</sup>, Action, Match, ORF-value<sup>5</sup>> и ORF состоит из одного или множества элементов ORF с совпадающими значениями AFI/SAFI и ORF-Type. Фильтр ORF идентифицируется парой <AFI/SAFI, ORF-Type>.

Компонента AFI/SAFI обеспечивает грубый контроль за счёт выбора только тех маршрутов, в которых значения NLRI<sup>6</sup> соответствуют компоненте AFI/SAFI в фильтре ORF.

Компонента ORF-Type определяет содержимое поля ORF-value.

Компонента Action<sup>7</sup> управляет обслуживанием запросов ORF Request удаленным партнёром. В качестве действия могут служить операции ADD, REMOVE, REMOVE-ALL. Операция ADD добавляет элемент ORF в фильтр ORF удалённого партнёра, REMOVE удаляет ранее установленный для удалённого партнёра элемент ORF, а REMOVE-ALL удаляет все ранее установленные для заданного ORF элементы.

Компонента Match используется для управления действиями на уровне элемента ORF и может принимать значения PERMIT или DENY. Значение PERMIT используется для запроса у партнёра передачи обновлений для маршрутов, соответствующих записи ORF. Значение DENY используется для запроса у партнёра фильтрации (отказа от передачи) обновлений, соответствующих элементу ORF.

При определении ORF конкретные правила соответствия для данного ORF **должны** быть заданы так, чтобы не возникало неоднозначностей при определении элемента ORF, по отношению к которому проверяется соответствие при прохождении маршрута через ORF.

<sup>1</sup>Outbound Route Filters - выходные фильтры маршрутов.

<sup>2</sup>Address Family Identifier.

<sup>3</sup>Subsequent Address Family Identifier.

<sup>4</sup>Тип ORF.

<sup>5</sup>Значение ORF.

<sup>6</sup>Network Layer Reachability Information - информация о доступности на сетевом уровне.

<sup>7</sup>Действие.

## 4. Передача элементов ORF в BGP

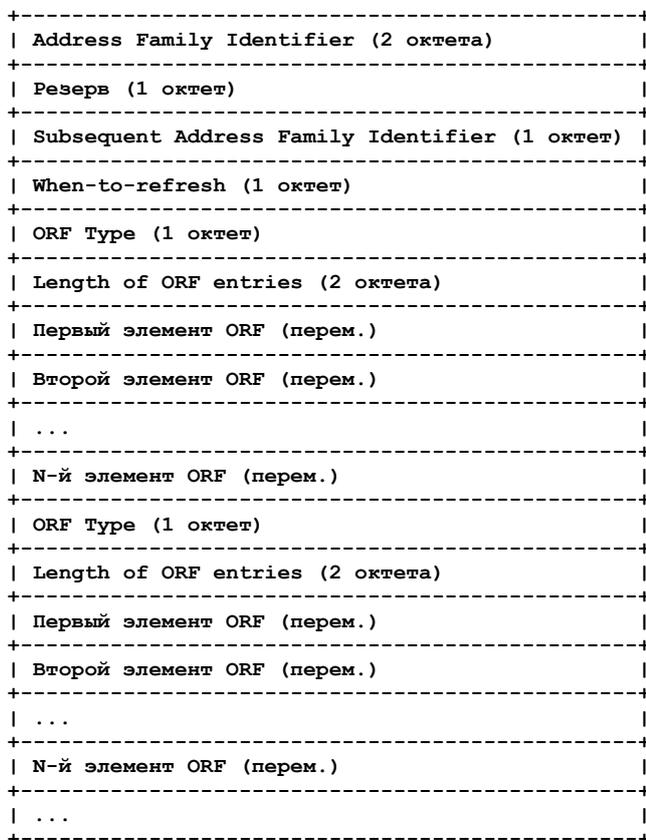


Рисунок 1. Передача элементов ORF в сообщении ROUTE-REFRESH.

Элементы ORF передаются в сообщениях BGP ROUTE-REFRESH [BGP-RR].

Узел BGP может отличать входящие сообщения ROUTE-REFRESH с одним или несколькими элементами ORF от обычных сообщений ROUTE-REFRESH с помощью поля Message Length<sup>1</sup> в заголовке сообщения BGP.

В одном сообщении ROUTE-REFRESH **может** содержаться множество элементов ORF для одного или множества фильтров ORF, при условии, что для всех этих элементов значения AFI/SAFI совпадают.

С точки зрения кодирования каждый элемент ORF состоит из общей части и зависимой от типа части, как показано на рисунках 1 и 2.

Общая часть включает поля <AFI/SAFI, ORF-Type, Action, Match> и представляется следующим образом:

Компонента AFI/SAFI элемента ORF представляется полями AFI/SAFI сообщения ROUTE-REFRESH.

Вслед за компонентой AFI/SAFI размещается 1-октетное поле When-to-refresh<sup>2</sup>, которое может принимать значения IMMEDIATE (0x01) или DEFER (0x02). Семантика значений IMMEDIATE и DEFER обсуждается ниже в параграфе «Функционирование».

Вслед за полем When-to-refresh помещается один или множество ORF, сгруппированных по ORF-Type.

Компонента ORF-Type представляет 1 октетом.

Компонента Length of ORF entries представляет собой 2-октетное поле, содержащую общий размер последующих однотипных элементов ORF в октетах.

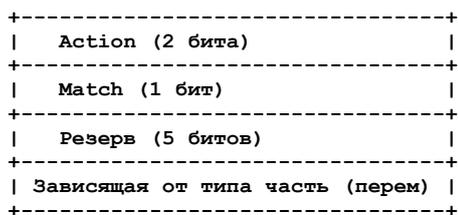


Рисунок 2. Представление записи ORF.

Остальные компоненты общей части кодируются в первом октете каждого элемента ORF (отсчёт от старшего бита), как показано на рисунке 2.

Поле Action занимает 2 бита и может принимать значения 0 (ADD), 1 (REMOVE) и 2 (REMOVE-ALL).

Поле Match занимает 1 бит. Значение 0 означает операцию PERMIT, а 1 - DENY. Это поле имеет смысл только в тех случаях, когда в поле Action указано значение ADD или REMOVE.

Резервное поле занимает 5 битов и должно содержать нулевые значения при передаче и игнорироваться на приёмной стороне.

<sup>1</sup>Размер сообщения.

<sup>2</sup>Когда обновлять.

Если компонента Action записи ORF задаёт значение REMOVE-ALL, данный элемент содержит только общую часть.

## 5. Возможность выходной фильтрации маршрутов

Узел BGP, желающий получать элементы ORF от своего партнёра, или узел BGP, желающий передавать элементы ORF своему партнёру анонсирует поддержку Outbound Route Filtering Capability, как описано ниже.

Outbound Route Filtering Capability<sup>1</sup> представляет собой новую возможность BGP<sup>2</sup> [BGP-CAP], определяемую следующим образом:

Capability code: 3

Capability length: переменное значение

Capability value: один или множество элементов фильтрации, как показано на рисунке 3.

```

+-----+
| Address Family Identifier (2 октета) |
+-----+
| Резерв (1 октет) |
+-----+
| Subsequent Address Family Identifier (1 октет) |
+-----+
| Number of ORFs (1 октет) |
+-----+
| ORF Type (1 октет) |
+-----+
| Send/Receive (1 октет) |
+-----+
| ... |
+-----+
| ORF Type (1 октет) |
+-----+
| Send/Receive (1 октет) |
+-----+

```

Рисунок 3. Представление Outbound Route Filtering Capability.

Значения полей описаны ниже.

### Address Family Identifier (AFI)

Смысл этого поля совпадает с описанным в [BGP-MP].

### Subsequent Address Family Identifier (SAFI)

Смысл этого поля совпадает с описанным в [BGP-MP].

### Number of ORF Types

Это поле содержит количество типов фильтров в последующих полях сообщения.

### ORF Type

Это поле указывает тип ORF.

### Send/Receive

Это поле показывает желаемую роль данного узла для указанного типа ORF - 1 означает желание узла принимать элементы ORF от своего партнёра, 2 говорит о намерении передавать элементы ORF, а 3 - о намерении принимать и передавать.

## 6. Функционирование

Узлу BGP, желающему получать элементы ORF от своего партнёра или передавать элементы ORF своему партнёру **следует** анонсировать партнёру возможность фильтрации маршрутов (Outbound Route Filtering Capability) с использованием механизма BGP Capabilities [BGP-CAP].

Узел BGP, реализующий выходную фильтрацию маршрутов, **должен** поддерживать сообщения BGP ROUTE-REFRESH в соответствии с [BGP-RR]. Узел BGP, анонсирующий партнёру выходную фильтрацию маршрутов с использованием BGP Capabilities [BGP-CAP], не анонсирует этому партнёру BGP Route Refresh Capability.

Рассмотрим узел BGP, который анонсирует Outbound Route Filtering Capability, указывая своё желание получать от партнёра определённый набор <AFI/SAFI, ORF-Type>, и получает анонсы Outbound Route Filtering Capability, показывающие, что партнёр передаёт определённый набор <AFI/SAFI, ORF-Type> данному узлу. Если для данных значений AFI/SAFI пересечение двух анонсируемых множеств не пусто, узлу BGP **не следует** анонсировать своему партнёру никаких маршрутов с данными AFI/SAFI до получения от этого партнёра сообщения ROUTE-REFRESH с данными AFI/SAFI; это сообщение может не включать элементов ORF или включать один или множество элементов ORF и поле When-to-refresh = IMMEDIATE. С другой стороны, если для данных AFI/SAFI пересечение двух множеств пусто, узел **должен** следовать обычным процедурам BGP.

Узел BGP может передавать своему партнёру сообщение ROUTE-REFRESH с одним или множеством элементов ORF только в тех случаях, когда этот партнёр передал данному узлу анонс Outbound Route Filtering Capability, показывающий желание получать элементы ORF, а сам узел анонсировал Outbound Route Filtering Capability с указанием желания передавать партнёру элементы ORF. Сообщение может содержать только элементы ORF с <AFI/SAFI, ORF-type>, которые партнёр желает получать в соответствии с полученным от него анонсом Outbound Route Filtering Capability.

Когда узел BGP получает от своего партнёра сообщение ROUTE-REFRESH с одним или множеством элементов ORF, он выполняет перечисленные ниже операции. Если значения <AFI/SAFI, ORF-type> в сообщении не соответствуют значениям <AFI/SAFI, ORF-type>, которые узел желает получать от партнёра (как было указано в анонсе Outbound Route Filtering Capability), соответствующие элементы ORF в полученном сообщении игнорируются. При совпадении

<sup>1</sup>Фильтрация маршрутов на выходе.

<sup>2</sup>BGP Capability.

значений узел изменяет соответствующие ORF, полученные ранее, согласно элементам ORF из принятого сообщения. Если любое из полей элемента ORF в сообщении содержит нераспознанное значение, соответствующий фильтр ORF, полученный ранее, полностью удаляется.

Если компонента Action элемента ORF имеет значение REMOVE, но полученный ранее фильтр ORF не содержит указанного элемента, запись ORF в сообщении игнорируется.

Элементы ORF со значениями REMOVE или REMOVE-ALL не могут удаляться локально сконфигурированными выходными фильтрами маршрутов.

Если поле When-to-refresh содержит значение IMMEDIATE, после обработки всех элементов ORF, содержащихся в сообщении, узел повторно анонсирует партнёру маршруты из Adj-RIB-Out, связанные с партнёром., которые имеют такие же значения AFI/SAFI, какие были получены в сообщении, и принимает во внимание все элементы ORF для значений AFI/SAFI, принятых от партнёра. Узел **должен** повторно анонсировать все маршруты, на которые оказывают влияние элементы ORF из принятого сообщения, и **может** также реанонсировать маршруты, на которые элементы ORF из сообщения не воздействуют.

Если When-to-refresh = DEFER, после обработки всех элементов ORF в сообщении узел отказывается от реанонсирования партнёру маршрутов из Adj-RIB-Out, связанных с партнёром., который имеет такие же значения AFI/SAFI, что были получены в сообщении, и принимает во внимание все элементы ORF, полученные от партнёра, до тех пор пока не будет принято следующее сообщение ROUTE-REFRESH с такими же значениями AFI/SAFI, но без элементов ORF или с одним или множеством элементов ORF и When-to-refresh = IMMEDIATE.

Если узел получает от партнёра сообщение ROUTE-REFRESH без элементов ORF, этот узел передаёт партнёру все маршруты из Adj-RIB-Out, связанные с партнёром., для которых значения AFI/SAFI совпадают с полученными в сообщении, и принимает во внимание все ранее принятые от партнёра ORF (если таковые имеются).

Набор элементов ORF, которые узел передаёт партнёру, выражает локальные предпочтения узла, которые этот партнёр может принимать или не принимать во внимание.

В течение сеанса BGP узел **может** передавать партнёру множество элементов ORF.

После того, как узел BGP меняет элементы ORF, переданные ранее партнёру, он **должен** передать этому партнёру обновлённые элементы ORF с (a) When-to-refresh = IMMEDIATE или (b) When-to-refresh = DEFER с последующим обычным сообщением ROUTE-REFRESH. Второй вариант **должен** использоваться узлом в тех случаях, когда имеются другие изменения в политике (в дополнение к элементам ORF), требующие реанонсирования партнёру всех маршрутов.

Время жизни фильтров ORF ограничивается продолжительностью сессии BGP, в которой происходил обмен ORF.

Фильтр ORF удаляется при удалении последнего элемента ORF (с помощью REMOVE-ALL или последовательности REMOVE).

Если отдельный маршрут, поддерживаемый узлом BGP, не соответствует ни одному элементу ORF ни в одном из (непустых) фильтров ORF, связанных с определенным партнёром., такой маршрут **не следует** анонсировать данному партнёру.

Если узел BGP поддерживает множество ORF с разными ORF-Type для одного партнёра, решение об анонсировании маршрута такому партнёру принимается путём просмотра маршрута всеми ORF и объединения полученных результатов (при объединении PERMIT и DENY результатом будет DENY).

## 7. Согласование с IANA

В этом документе определяется новая возможность BGP<sup>1</sup> - Outbound Route Filtering Capability. Значение Capability Code для Outbound Route Filtering Capability равно 3.

Как указано в этом документе, элемент ORF содержит поле ORF-Type, для которого агентство IANA создало и поддерживает реестр BGP Outbound Route Filtering (ORF) Types.

IANA поддерживает и регистрирует значения поля ORF-Type в соответствии с приведёнными ниже условиями:

- Значение ORF-Type = 0 является резервным.
- Значения ORF-Type от 1 до 63 выделяются IANA с использованием процедуры Standards Action, определённой в RFC 5226 [RFC5226], или процедуры Early IANA Allocation, определённой в RFC 4020 [RFC4020].
- Значения ORF-Type от 64 до 127 выделяются IANA с использованием процедуры First Come First Served, определённой в RFC 5226 [RFC5226].
- Значения ORF-Type от 128 до 255 являются специфическими для производителей и не распределяются IANA.

## 8. Вопросы управления

Объекты управления для фильтров BGP ORF будут определены в отдельном документе. Однако предполагается, что будут определены следующие объекты:

Объект ORF Capability, которые описывает ORF Capability, передаваемые в сессии BGP, должен включать типы ORF и значения Send/Receive, анонсируемые и принимаемые узлом BGP.

Объект ORF должен включать элементы ORF каждого фильтра ORF, передаваемого и принимаемого узлом BGP.

## 9. Вопросы безопасности

Данное расширение BGP не отражается на вопросах безопасности, рассмотренных в [BGP-4].

<sup>1</sup>BGP Capability.

## 10. Благодарности

Часть материалов этого документа является адаптацией предложения для селективных обновлений, подготовленного Yakov Rekhter, Kannan Varadhan и Curtis Villamizar.

## 11. Нормативные документы

- [BGP-4] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", [RFC 4271](#), January 2006.
- [BGP-MP] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", [RFC 4760](#), January 2007.
- [BGP-CAP] Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", [RFC 3392](#), November 2002.
- [BGP-RR] Chen, E., "Route Refresh Capability for BGP-4", [RFC 2918](#), September 2000.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, [RFC 2119](#), March 1997.
- [RFC4020] Kompella, K. and A. Zinin, "Early IANA Allocation of Standards Track Code Points", BCP 100, [RFC 4020](#), February 2005.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, [RFC 5226](#), May 2008.

## Адреса авторов

### Enke Chen

Cisco Systems, Inc.  
170 W. Tasman Dr.  
San Jose, CA 95134  
Email: [enkechen@cisco.com](mailto:enkechen@cisco.com)

### Yakov Rekhter

Juniper Networks  
1194 N. Mathilda Ave  
Sunnyvale, CA 94089  
Email: [yakov@juniper.net](mailto:yakov@juniper.net)

## Перевод на русский язык

Николай Малых

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

## Полное заявление авторских прав

Copyright (C) The IETF Trust (2008).

К этому документу применимы права, лицензии и ограничения, указанные в BCP 78, и, за исключением указанного там, авторы сохраняют свои права.

Этот документ и содержащаяся в нем информация представлены "как есть" и автор, организация, которую он/она представляет или которая выступает спонсором (если таковой имеется), Internet Society и IETF отказываются от каких-либо гарантий (явных или подразумеваемых), включая (но не ограничиваясь) любые гарантии того, что использование представленной здесь информации не будет нарушать чьих-либо прав, и любые предполагаемые гарантии коммерческого использования или применимости для тех или иных задач.

### 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](mailto:ietf-ipr@ietf.org).