Internet Engineering Task Force (IETF)
Request for Comments: 8402
Category: Standards Track
ISSN: 2070-1721

C. Filsfils, Ed.
S. Previdi, Ed.
L. Ginsberg
Cisco Systems, Inc.
B. Decraene
S. Litkowski
Orange
R. Shakir
Google, Inc.

July 2018

Архитектура маршрутизации по сегментам

Segment Routing Architecture

Тезисы

Маршрутизация по сегментам (SR[1]) использует парадигму маршрутизации, заданной отправителем (source routing). Узел направляет пакет с помощью упорядоченного списка инструкций, называемых сегментами. Сегмент может представлять инструкцию, основанная на топологии или услугах. Семантика сегмента может быть локальной для узла SR или глобальной в рамках домена SR. Маршрутизация по сегментам обеспечивает механизм, который позволяет ограничивать потоки конкретным топологическим путем при поддержке состояний на уровне потока лишь на входных узлах домена SR.

SR может напрямую применяться в архитектуре MPLS без изменения уровня пересылки. Сегменты представляются в виде меток MPLS, а упорядоченный список сегментов — в виде стека меток. Обрабатываемый сегмент находится на вершине стека и после завершения обработки соответствующая метка выталкивается из стека.

SR можно использовать с архитектурой IPv6 с новым типом заголовка маршрутизации. Сегмент представляется в виде адреса IPv6, а упорядоченный список сегментов — в виде упорядоченного списка адресов IPv6 в заголовке маршрутизации. Активный сегмент указывается адресом получателя (DA[2]) пакета. Следующий активный сегмент задается указателем в новом заголовке маршрутизации.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[3] и представляет согласованный взгляд сообщества IETF. Документ прошел открытое обсуждение и был одобрен для публикации IESG[4]. 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 https://www.rfc-editor.org/info/rfc8402.

Оглавление

[1]Segment Routing.
[2]Destination Address.
[3]Internet Engineering Task Force.
[4]Internet Engineering Steering Group.

1. Введение

Маршрутизация по сегментам (SR) использует парадигму маршрутизации, заданной отправителем (source routing). Узел направляет пакет с помощью упорядоченного списка инструкций, называемых сегментами. Сегмент может представлять инструкцию, основанная на топологии или услугах. Семантика сегмента может быть локальной для узла SR или глобальной в рамках домена SR. Маршрутизация по сегментам обеспечивает механизм, который позволяет ограничивать потоки конкретным топологическим путем при поддержке состояний на уровне потока лишь на входных узлах домена SR.

Сегменты часто указывают их идентификаторами SID[1].

Сегмент может быть связан с топологической инструкцией. Топологический локальный сегмент может инструктировать узел пересылать пакет через конкретный выходной интерфейс. Топологический глобальный сегмент может инструктировать домен SR пересылать пакет через конкретный путь к получателю. Для этого же получателя могут существовать другие сегменты с другими целями путей (например, минимизация метрики или набор ограничений).

Сегмент может быть связан с сервисной инструкцией (например, пакет следует обрабатывать в контейнере или виртуальной машине (VM[2]), связанной с сегментом). Сегмент может быть связан с трактовкой QoS (например, предоставление для пакетов данного сегмента пропускной способности x Мбит/с).

Архитектура SR поддерживает любые типы связанных с сегментами инструкций.

Архитектура SR поддерживает любой тип уровня управления — распределенный, централизованный или гибридный.

В распределенном варианте выделение сегментов и сигнализация обеспечиваются протоколом IS-IS, OSPF или BGP. Узел сам решает вопрос направления пакетов в SR Policy (например, заранее рассчитанная локальная защита [RFC8355]). Узел индивидуально рассчитывает SR Policy.

В централизованном варианте сегменты выделяются и создаются контроллером SR. Контроллер SR решает, какие узлы должны направлять пакеты в соответствии с правилами заданной отправителем маршрутизации. Контроллер SR рассчитывает правила заданной отправителем маршрутизации. Архитектура SR не ограничивает способы программирования сети контроллером. Возможными вариантами такого программирования являются протоколы NETCONF[3], PCEP[4] и BGP. Архитектура SR не ограничивает число контроллеров SR. В частности, может применяться множество контроллеров для программирования одного домена SR. Архитектура SR позволяет этим контроллерам обнаруживать экземпляры SID и определять узлы, где они созданы, а также определять доступность на узлах локальных (SRLB) и глобальных (SRGB) меток.

В гибридном варианте базовый распределенный уровень управления дополняется центральным контроллером. Например, при размещении адресата за пределами домена IGP контроллер SR может рассчитать SR Policy от имени узла IGP. Архитектура SR не ограничивает способы взаимодействия узлов, участвующих в управлении, с контроллером SR. Возможными вариантами являются протоколы PCEP и BGP.

Хосты **могут** быть частью домена SR. Центральный контроллер может информировать хосты о правилах путем их выталкивания на хосты (pushing) или путем ответов на запросы хостов.

Экземпляры архитектуры SR могут создаваться для различных уровней данных. В этом документе рассматриваются два таких экземпляра - SR для MPLS (SR-MPLS) и SR для IPv6 (SRv6).

SR можно применять непосредственно к архитектуре MPLS без изменения уровня пересылки [SR-MPLS]. Сегменты представляются в виде меток MPLS. Экземпляры SR Policy создаются в форме стека меток. Обрабатываемым (активным) сегментом является сегмент на вершине стека. По завершению обработки сегмента соответствующая метка выталкивается из стека.

SR можно применять в архитектуре IPv6 с использованием нового типа заголовков маршрутизации, называемого заголовком SR (SRH[5]) [IPv6-SRH]. Связанная с сегментом инструкция представляется в виде адреса IPv6. Сегменты

[1]Segment Identifier.
[2]Virtual Machine.
[3]Network Configuration Protocol — протокол настройки конфигурации сети.
[4]Path Computation Element Communication Protocol — протокол коммуникаций между элементами расчета путей.
[5]SR Header.

SRv6 называют также SRv6 SID. Экземпляр SR Policy создается в форме упорядоченного списка SRv6 SID в заголовке маршрутизации. Активный сегмент указывается адресом получателя (DA) в пакете. Следующий активный сегмент задается указателем SegmentsLeft (SL) в SRH. По завершении обработки SRv6 SID значение SL декрементируется и в DA копируется следующий сегмент. Когда пакет направляется SR Policy, в него добавляется соответствующий заголовок SRH.

В контексте распределенного уровня управления на базе IGP определяется два топологических сегмента - IGP-Adjacency и IGP-Prefix.

В контексте распределенного уровня управления на базе BGP определяется два топологических сегмента - BGP peering и BGP-Prefix.

Головная точка (headend) SR Policy связывает SID (сегмент Binding или BSID) со своей политикой. Когда головная точка получает пакет, активный сегмент которого соответствуют BSID локальной политики SR, она направляет пакет в SR Policy.

Этот документ определяет сегменты IGP, BGP и Binding для уровней данных SR-MPLS и SRv6.

> Примечание. Этот документ определяет архитектуру SR, включая определения базовых объектов и функций, а также общее описание устройства. Документ **не** определяет способов реализации архитектуры, которые описаны во множестве других документов, часть которых для удобства перечислена в разделе ссылок.

2. Терминология

Ключевые слова **необходимо** (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 BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

SR-MPLS
: Экземпляр SR для уровня данных MPLS.

SRv6
: Экземпляр SR для уровня данных IPv6.

Segment - сегмент
: Инструкция, выполняемая узлом для входящего пакета (например, пересылка по кратчайшему пути к адресату, пересылка через конкретный интерфейс или доставка определенному экземпляру приложения или сервиса).

SID
: Идентификатор сегмента. Отметим, что термин SID часто используется вместо термина «сегмент», хотя технически это не совсем точно.

SR-MPLS SID
: Метка MPLS или значение индекса в пространстве меток MPLS, явно связанные с сегментом.

SRv6 SID
: Адрес IPv6, явно связанный с сегментом.

Segment Routing domain (SR domain) – домен SR
: Множество узлов, участвующих в модели заданной отправителем маршрутизации. Эти узлы могут быть соединены в одну физическую инфраструктуру (например, сеть сервис-провайдера). Узлы могут также быть связаны удаленными соединениями (например, VPN организации или наложенная сеть). При использовании множества протоколов домен SR обычно будет включать все экземпляры сетевых протоколов. Однако в некоторых случаях может быть желательно разделение сети на множество доменов SR, каждый из которых включает один или несколько экземпляров протоколов. Предполагается, что все узлы в домене SR имеют общее администрирование.

Active Segment – активный сегмент
: Сегмент, используемый принимающим маршрутизатором для обработки пакета. Для MPLS это верхняя метка в стеке, для IPv6 — адрес получателя [IPv6-SRH].

PUSH - вталкивание
: Операция вставки сегмента на вершину списка сегментов. Для SR-MPLS вершиной списка является верхняя (внешняя) метка в стеке. Для SRv6 вершина списка сегментов представлена первым сегментом в заголовке SRH, как определено в [IPv6-SRH].

NEXT – следующий сегмент
: При завершении обработки активного сегмента NEXT является операцией проверки следующего сегмента, который становится активным. В SR-MPLS операция NEXT реализуется выталкиванием (POP) верхней метки, в SRv6 — копированием следующего сегмента из SRH в поле адреса получателя заголовка IPv6.

CONTINUE – продолжение сегмента
: Активный сегмент не завершен, поэтому он остается активным. В SR-MPLS операция CONTINUE реализуется заменой (SWAP) верхней метки [RFC3031], в SRv6 это обычная операция пересылки IPv6 в соответствии с адресом получателя IPv6.

SR Global Block (SRGB) – глобальный блок SR
: Набор глобальных сегментов в домене SR. Если узел участвует в нескольких доменах SR, для каждого из них будет присутствовать блок SRGB. В SR-MPLS блок SRGB является локальным свойством узла и указывает множество локальных меток, зарезервированных для глобальных сегментов. В SR-MPLS настоятельно рекомендуется использовать одинаковые блоки SRGB на всех узлах домена SR. Это упрощает работу и поиск неисправностей, поскольку на каждом узле одна и та же метка будет представлять один и тот же сегмент. В SRv6 блок SRGB представляет собой набор глобальных SRv6 SID в домене SR.

SR Local Block (SRLB) – локальный болк SR
: Локальное свойство узла SR. Если узел участвует в нескольких доменах SR, используется один блок SRLB для каждого домена SR. В SR-MPLS блок SRLB представляет собой набор локальных меток, зарезервированных для локальных сегментов. В SRv6 блок SRLB представляет собой набор локальных адресов IPv6, зарезервированных для локальных SRv6 SID. В управляемой контроллерами сети некоторые контроллеры или приложения могут использовать уровень управления для определения доступного набора локальных сегментов.

Global Segment – глобальный сегмент
Сегмент, являющийся частью SRGB домена. Связанная с сегментом инструкция определяется на уровне домена SR. Типичным примером глобального сегмента является топологический кратчайший путь к данному адресату внутри домена SR.

Local Segment – локальный сегмент
В SR-MPLS это локальная метка вне SRGB. Это может быть часть явно анонсируемого SRLB. В SRv6 это может быть любой адрес IPv6 (т. е. адрес может быть частью SRGB, но используется так, что его значимость локальна). Инструкция, связанная с сегментом, определяется на уровне узла.

IGP Segment – сегмент IGP
Базовое имя для сегмента, присоединенного к части информации, анонсируемой link-state IGP (например, префикс или смежность IGP).

IGP-Prefix Segment – сегмент IGP-Prefix
Сегмент IGP-Prefix является сегментом IGP, представляющим префикс IGP. Когда сегмент IGP-Prefix является глобальным в рамках экземпляра или топологии SR IGP, он определяет инструкцию для пересылки пакета по пути, рассчитанному с использованием алгоритма маршрутизации, заданного в поле algorithm, для топологии и экземпляра IGP, где этот сегмент анонсируется. Используется также термин prefix segment (сегмент префикса).

Prefix-SID
Идентификатор SID для сегмента IGP-Prefix.

IGP-Anycast Segment - сегмент IGP-Anycast
Сегмент IGP-Anycast является сегментом IGP-Prefix, который указывает префикс anycast, анонсируемый набором маршрутизаторов.

Anycast-SID
Идентификатор SID для сегмента IGP-Anycast.

IGP-Adjacency Segment – сегмент IGP-Adjacency
Сегмент IGP-Adjacency является сегментом IGP, присоединенным к однонаправленной смежности или набору таких смежностей. По умолчанию сегмент IGP-Adjacency является локальным (если явно не анонсируется иное) для анонсирующего его узла. Называется также Adj-SID.

Adj-SID
Идентификатор SID для сегмента IGP-Adjacency.

IGP-Node Segment – сегмент IGP-Node
Сегмент IGP-Node является сегментом IGP-Prefix, который указывает конкретный маршрутизатор (например, loopback). Называется также Node Segment 9сегмент узла).

Node-SID
Идентификатор SID для сегмента IGP-Node.

SR Policy – правила (политика) SR
Упорядоченный список сегментов. Головная точка SR Policy направляет пакеты в SR Policy. Список сегментов может быть задан явно в SR-MPLS как стек меток и в SRv6 как упорядоченный список SRv6 SID. Кроме того, список сегментов рассчитывается на основе адресата и набора параметров оптимизации и ограничений (например, задержка, сродство, SRLG и т. п.). Расчет может выполняться локально или передаваться серверу PCE. SR Policy может настраиваться оператором, а также обеспечиваться протоколом NETCONF [RFC6241] или PCEP [RFC5440]. Политика SR может применяться для организации трафика (TE[1]), решения задач OAM[2] или быстрой смены маршрутов (FRR[3]).

Segment List Depth – размер списка сегментов
Число сегментов в SR Policy. Объект, создающий экземпляр SR Policy на узле N, должен быть способен определить возможности sdepth-insertion для узла N. Например, анонсирование свойства PCEP SR, описанное в [PCEP-SR-EXT], является одним из способов обнаружения возможности.

Forwarding Information Base (FIB) – база данных о пересылке
Таблица пересылки узла.

3. Сегменты Link-State IGP

В домене SR узел IGP с поддержкой SR анонсирует сегменты для своих подключенных префиксов и смежностей (соседств). Эти сегменты называют сегментами IGP или IGP SID. Они играют важную роль в SR и позволяют выразить любой путь через домен SR. Такой путь выражается одним сегментом IGP или списком из множества сегментов IGP.

Для анонсирования сегментов IGP требуется расширение протоколов IGP, основанных на состоянии каналов. Эти расширения определены в [ISIS-SR-EXT], [OSPF-SR-EXT] и [OSPFv3-SR-EXT].

3.1. Сегмент IGP-Prefix (Prefix-SID)

Сегмент IGP-Prefix является сегментом IGP, присоединенным к префиксу IGP. Сегмент IGP-Prefix является глобальным (если явно не указано иное) в домене SR. Контекст сегмента IGP-Prefix включает префикс, топологию и алгоритм. **Может** быть выделено множество SID для одного префикса, пока триплеты <prefix, topology, algorithm> являются уникальными.

Множество экземпляров и топологий определены для IS-IS и OSPF в [RFC5120], [RFC8202], [RFC6549] и [RFC4915].

3.1.1. Алгоритм Prefix-SID

SR поддерживает использование множества алгоритмов маршрутизации, т. е. может поддерживаться множество разных расчетов кратчайшего пути с учетом ограничений. Идентификатор алгоритма включается в анонс Prefix-SID. Определяющий алгоритм документ должен включать спецификацию расчета пути для этого алгоритма.

Данный документ определяет два алгоритма.

[1]Traffic Engineering.
[2]Operations, Administration, and Maintenance — операции, администрирование, обслуживание.
[3]Fast Reroute.

- По кратчайшему пути (SPF[1]). Этот алгоритм используется по умолчанию. Пакет пересылается с использованием общепринятого алгоритма SPF, знающего о ECMP[2], который реализуется протоколами IGP. Однако промежуточным точкам явно разрешено применять другие алгоритмы пересылки в соответствии с локальной политикой. Алгоритм SPF фактический является используемым по умолчанию в большинстве современных сетей, где локальные правила могут переопределять решение SPF.

- Строго по кратчайшему пути (Strict-SPF). Этот алгоритм требует пересылать пакет в соответствии с алгоритмом SPF, знающим о ECMP, и инструктирует все маршрутизаторы на пути игнорировать любые локальные правила, переопределяющие решение SPF. Идентификатор SID, анонсируемый с алгоритмом Strict-SPF, обеспечивает неизменность пути SPF, по которому пересылается пакет. Отметим, что механизмы быстройсмены маршрутов (FRR) [RFC5714] совместимы с этим алгоритмом. Иными словами, пакет, полученный с Strict-SPF SID, может быть перемаршрутизирован механизмом FRR. Strict-SPF использует такую же топологию, как алгоритм SPF. Обычно узлы, не поддерживающие Strict-SPF, не будут создавать записей пересылки для этого алгоритма. Ограничение топологии лишь узлами, поддерживающими этот алгоритм, не создает желаемых путей пересылки, поскольку желаемое поведение состоит в следовании маршрутам, рассчитанным по алгоритму SPF. Поэтому исходному узлу SR **недопустимо** использовать SR Policy с сегментом Strict-SPF, если путь проходит через узлы, не поддерживающие алгоритм Strict-SPF.

Сегмент IGP-Prefix указывает путь к соответствующему префиксу, рассчитанный с использованием привязанного алгоритма. Предполагается, что пакет внесенный где-либо внутри домена SR с активным Prefix-SID, будет пересылаться по пути, рассчитанному с использованием указанного алгоритма. Для этого требуется полносвязная топология маршрутизаторов, поддерживающих этот алгоритм.

3.1.2. SR-MPLS

Когда SR используется с уровнем данных MPLS, идентификаторы SID являются метками MPLS или индексами в пространстве меток MPLS (SRGB или SRLB).

По возможности рекомендуется настраивать идентичные блоки SRGB на всех узлах домена SR. Это упрощает поиск неисправностей, поскольку с одним префиксом связывается одна и та же метка на всех узлах. Кроме того, это упрощает поддержку адресации anycast, как описано в параграфе 3.3.

Ниже перечислены аспекты поведения, связанные с SR на основе уровня данных MPLS.

- Расширение сигнализации IGP для сегмента IGP-Prefix включает флаг для указания непосредственно подключенным соседям операции NEXT или CONTINUE при обработке SID. Это поведение эквивалентно Penultimate Hop Popping (NEXT) или Ultimate Hop Popping (CONTINUE) в MPLS.

- Prefix-SID выделяется в форме метки MPLS (или индекса в SRGB), подобно выделению адреса IP. Обычно выделение Prefix-SID происходит в соответствии с политикой оператора или NMS[3] и значение SID меняется очень редко.

- Хотя SR позволяет привязать к перфиксу IGP локальный сегмент, термины «сегмент IGP-Prefix» и Prefix-SID предполагают глобальный сегмент (т. е. SID определяется из анонсируемого SRGB). Это согласуется со всеми описанными примерами использования, которые требуют привязки к префиксам IGP глобальных сегментов.

- Процессу выделения **недопустимо** назначать один идентификатор Prefix-SID для разных префиксов.

- Если узел узнает Prefix-SID со значением, выходящим за пределы локально настроенного диапазона SRGB, этому узлу **недопустимо** использовать Prefix-SID и **следует** внести в журнал запись об ошибке в конфигурации.

- Если узел N анонсирует Prefix-SID SID-R для префикса R, который присоединен к N, и задает операцию CONTINUE для выполнения подключенными напрямую соседями, узел N **должен** поддерживать показанную ниже запись в FIB.

  Входящий активный сегмент: SID-R

  Входящая операция: NEXT

  Выходной интерфейс: NULL

- Удаленный узел M **должен** поддерживать приведенную ниже запись FIB для любого узнанного Prefix-SID SID-R, присоединенного к R.

  Входящий активный сегмент: SID-R

  Входящая операция: Если next-hop префикса R является источником (originator) R, а M дана инструкция удалить активный сегмент, выполняется операция NEXT. В противном случае выполняется CONTINUE.

  Выходной интерфейс: Интерфейс(ы) в направлении next-hop по пути, рассчитанному с использованием алгоритма, анонсированного с SID в направлении префикса R.

Поскольку Prefix-SID являются специфичными для данного алгоритма, связанный с алгоритмом трафик будет отбрасываться при поступлении на узел, который не поддерживает этот алгоритм (нет записи для пересылки, соответствующей входящей метке).

3.1.3. SRv6

При использовании SR с уровнем данных IPv6:

- Prefix-SID является адресом IPv6:

[1]Shortest Path First.
[2]Equal Cost Multipath — множество расноценных путей.
[3]Network Management System — система управления сетью.

- оператор **должен** явно создать экземпляр SRv6 SID. Адреса IPv6 по умолчанию не являются SRv6 SID.

Узел N, анонсирующий адрес IPv6 R, подходящий в качестве идентификатора сегмента, **должен** поддерживать приведенную ниже запись FIB.

Входящий активный сегмент: R

Входящая операция: NEXT

Выходной интерфейс: NULL

Отметим, что для пересылки в R не требуется записей FIB для префикса R в остальных маршрутизаторах. Пересылка может и большинстве случаев будет выполняться для более короткого префикса, включающего R.

Независимо от поддержки SR любой удаленный узел IPv6 будет поддерживать обычную (plain) запись IPv6 FIB для любого префикса представляющего или не представляющего сегмент. Это позволяет пересылать пакеты узлу, владеющему SID, даже узлам, не поддерживающим SR.

Для SRv6 возможна поддержка множества алгоритмов. Поскольку связанные с алгоритмами SID являются просто адресами IPv6, связанные с алгоритмом записи пересылки могут быть получены путем выделение узлом связанных с алгоритмом подсетей, к которым относятся связанные с алгоритмами SID.

Не поддерживающие алгоритм узлы могут по-прежнему иметь записи FIB, включающие относящийся к алгоритму адрес, даже в тех случаях, когда данный узел не рассчитывает связанного с алгоритмом пути. Это смягчается тем, что не поддерживающие данный алгоритм узлы не будут включаться в топологию, связанную со специфичным для алгоритма SPF. Поэтому трафик для связанных с алгоритмом адресатов обычно не будет проходить через исключенный узел. Если такой трафик будет приходить на узел и пересылаться им, он будет по-прежнему продвигаться в направлении адресата. Значение next-hop будет указывать поддерживающий алгоритм узел (в этом случае пакеты будут пересылаться по связанным с алгоритмом путям или обрасываться при отсутствии таких путей) или узел который **не** поддерживает данный алгоритм (в этом случае пакеты будут пересылаться по путям Algorithm 0 в направлении адресата).

3.2. Сегмент IGP-Node (Node-SID)

Сегмент IGP Node-SID **недопустимо** связывать с префиксом, которым владеет несколько маршрутизаторов в одном домене маршрутизации.

3.3. Сегмент IGP-Anycast (Anycast-SID)

Сегмент Anycast или Anycast-SID форсирует осведомленную об ECMP пересылку в направлении ближайшего узла набора anycast. Это полезно при создании правил организации трафика на макроуровне и механизмов защиты.

Сегментам IGP-Anycast **недопустимо** указывать на конкретный узел.

Внутри группы anycast все маршрутизаторы домена SR **должны** анонсировать для одного SID один и тот же префикс.

3.3.1. Anycast-SID в SR-MPLS

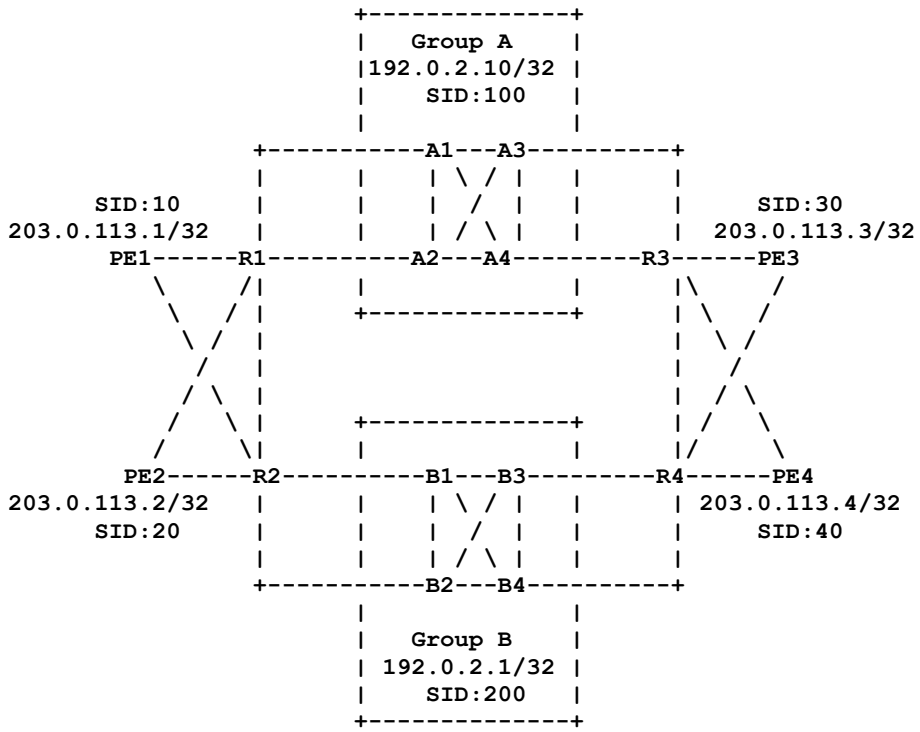

Рисунок 1. Группы транзитных устройств.

На рисунке 1 показан пример сети с двумя группами транзитных устройств. Группа A включает устройства {A1, A2, A3 и A4}. Для всех этих устройств используется anycast-адрес 192.0.2.10/32 и Anycast-SID 100.

Группа B включает устройства {B1, B2, B3 и B4} с anycast-адресом 192.0.2.1/32 и Anycast-SID 200. В этой топологии каждое краевое устройство PE (Provide Edge) имеет путь в группы A и B.

PE1 может выбрать конкретную группу транзитных устройств для передачи трафика из PE3 или PE4. Это будет выполняться путем вталкивания Anycast-SID выбранной группы в стек.

Обработка anycast и последующих сегментов требует особой осторожности.

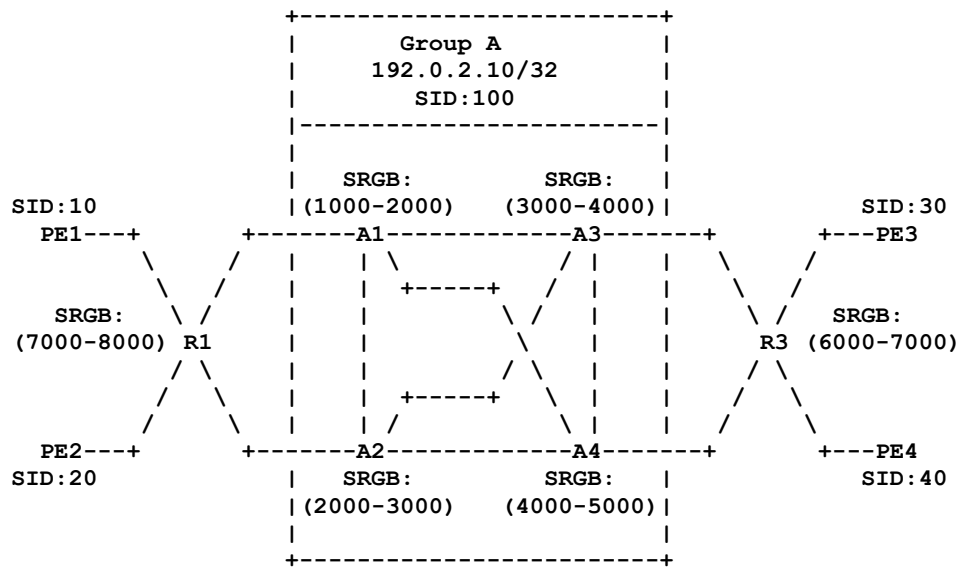

Рисунок 2. Транзитные пути через Anycast Group A.

Для случая MPLS в показанной выше топологии при необходимости передачи пакета от устройства PE1 (или PE2) устройству PE3 (или PE4) потребуется инкапсулировать пакет в данные (payload) MPLS с показанным ниже стеком меток.

- Метка, выделенная R1 для Anycast-SID 100 (внешняя).
- Метка, выделенная ближайшим маршрутизатором группы A для SID 30 (для получателя PE3).

В этом случае первую метку легко рассчитать. Однако по причине наличия в этой топологии более одного ближайшего устройства (A1 и A2) определение второй метки невозможно, если A1 и A2 не выделят одно и то же значение метки для одного префикса. Устройства A1 и A2 могут быть выпущены разными производителями. Если оба устройства не выделят одинаковые метки для SID 30, будет невозможно использовать anycast Group A в качестве транзитной anycast-группы в направлении PE3. Поэтому PE1 (или PE2) не сможет рассчитать подходящий стек меток для того, чтобы явно направить пакет через устройства группы A. То же самое будет происходить для устройств PE3 и PE4 при попытке передать пакет из PE1 или PE2.

Чтобы упростить использование сегмента anycast, рекомендуется настраивать идентичные блоки SRGB на всех узлах конкретной группы anycast. При использовании описанного выше метода расчет метки, следующей за сегментом anycast, становится простым.

Использование сегмента anycast без настройки одинаковых SRGB на всех узлах anycast-группы может приводить к ошибкам в маршрутизации (в среде MPLS VPN может возникать утечка трафика между VPN).

3.4. Сегмент IGP-Adjacency (Adj-SID)

Смежность формируется между локальным (т. е. анонсирующим отношения смежности в IGP) и удаленным (т. е. другой стороной отношений смежности) узлами. Локальный узел **должен** быть узлом IGP. Удаленный узел может быть смежным соседом IGP или несмежным соседом (например, смежность по пересылке [RFC4206]).

Пакет, инжектируемый в любой точке домена SR со списком сегментов {SN, SNL}, где SN - Node-SID узла N, SNL — Adj-SID, привязанный к N смежностью по каналу L, будет пересылаться по кратчайшему пути к N, а затем будет коммутироваться узлом N без учета кратчайшего пути IP в направлении канала L. Если Adj-SID указывает множество смежностей, узел N будут распределять трафик между элементами множества.

Аналогично при использовании глобального Adj-SID пакет, инжектированный в домен SR со списком сегментов {SNL}, где SNL -глобальный идентификатор Adj-SID, связанный узлом N со смежностью по каналу L, будет пересылаться по кратчайшему пути к N, а затем коммутироваться узлом N без учета кратчайшего пути IP в направлении канала L. Если Adj-SID указывает множество смежностей, узел N будут распределять трафик между элементами множества. Использование глобального Adj-SID позволяет уменьшить размер списка сегментов при выражении пути за счет дополнительного состояния (т. е. глобальный Adj-SID будет вставляться всеми маршрутизаторами области в их таблицы пересылки).

Сегмент IGP-Adjacency или Adj-SID форсирует коммутацию пакета от узла в направлении определенного интерфейса или набора интерфейсов. Это служит ключом к теоретическому доказательству того, что любой путь можно выразить в форме списка сегментов.

Представление Adj-SID включает набор флагов, поддерживаемых приведенную ниже функциональность.

- Право на защиту (например, с помощью IPFRR или MPLS-FRR). Защита позволяет в случае отказа интерфейсов, связанных с Adj-SID, пересылать пакеты по другому пути. Использование защиты безусловно определяется политикой, т. е. может быть или не быть желательным.
- Индикация локального или глобального действия Adj-SID. По умолчанию **следует** использовать локальную область действия.

- Индикация сохранения Adj-SID при перезапуске уровня управления. Сохранение является ключевым атрибутом, предотвращающим SR Policy от временной некорректности пересылки в результате повторного выделения Adj-SID.

Вес (как описано ниже) также связывается с анонсом Adj-SID.

Узлу **следует** выделять один идентификатор Adj-SID для каждой из своих смежностей.

Узел **может** выделять множество Adj-SID для одной смежности. Примером является поддержка Adj-SID с желательной и нежелательной защитой.

Узел **может** связать одие идентификатор Adj-SID со множеством смежносетй.

Для обеспечения возможности анонсировать в IGP все идентификаторы Adj-SID, представляющие отношения смежности IGP между парой узлов, **недопустимо** подавление параллельных смежностей протоколом IGP.

Когда узел связывает Adj-SID V с локальным каналом данных L, он **должен** установить в FIB приведенную ниже запись.

Входящий активный сегмент: V

Входящая операция: NEXT

Выходной интерфейс: L

Adj-SID предполагает пересылку пакетов через указанные Adj-SID смежности от анонсирующего Adj-SID маршрутизатора независимо от стоимости IGP/SPF. Инями словами, использование сегментов смжности переопределяет решение о маршрутизации, принятое алгоритмом SPF.

3.4.1. Параллельные смежности

Adj-SID могут применяться для представления набора параллельных интерфейсов между двумя смежными маршрутизаторами.

Узел **должен** создать запись FIB для любого локально инициированного Adj-SID со значением W, связанного с набором каналов B.

Входящий активный сегмент: W

Входящая операция: NEXT

Выходные интерфейсы: балансировка трафика между каналами данных набора B.

Когда параллельные смежности применяются и связаны с одним Adj-SID для оптимизации функции распределения нагрузки можно связать весовой коэффициент с идентификатором Adj-SID, анонсируемым для каждой смежности. Вес указывает вход (или систему SDN/оркестроки) коэффициента загрузки для параллельных смежностей. Как показано на рисунке 3, A и B соединены двумя параллельными отношениями смежности.

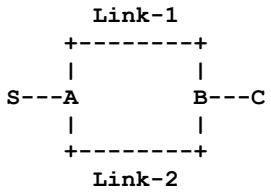

Рисунок 3. Параллельные каналы и Adj-SID.

Ужел A анонсирует Adj-SID и весовые коэффициенты

- Link-1: Adj-SID 1000, weight: 1
- Link-2: Adj-SID 1000, weight: 2

Узел S получает анонсы параллельных смежностей и понимает, что путем использования Adj-SID 1000 узла A будет распределять трафик между параллельными каналами (Link-1 и Link-2) в отношении 1:2 (т. е. через Link-2 будет передаваться вдвое больше пакетов по сравнению с Link-1).

3.4.2. Сегменты смежности ЛВС

В подсетях ЛВС протоколы link-state определяют концепцию назначенного маршрутизатора (DR[1] в OSPF) или назначенной промежуточной системы (DIS[2] в IS-IS), которые передают лавинные рассылки в широковещательных подсетях и описывают топологию ЛВС в специальных маршрутных обновлениях (OSPF Type2 LSA или IS-IS Pseudonode LSP).

Сложность заключается в том, что каждый маршрутизатор анонсирует лишь свою связность с DR/DIS, а не каждого отдельного узла в ЛВС. Поэтому нужны дополнительные механизмы протоколов (IS-IS и OSPF) для того. Чтобы каждый маршрутизатор в ЛВС анонсировал Adj-SID, связанный с каждым соседом в LAN.

3.5. Взаимодействия между областями

В приведенном ниже примере предполагается, что все области (area) являются частями одного домена SR.

На рисунке 4 предполагается уровень управления IPv6 и уровень данных MPLS.

В области 2 узел Z выделяет Node-SID 150 для своего локального префикса IPv6 2001:DB8::2:1/128.

[1]Designated Router.
[2]Designated Intermediate System.

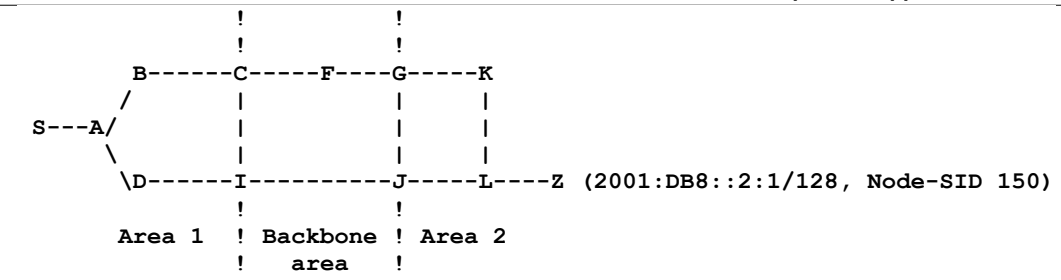

Рисунок 4. Пример топологии Inter-Area.

Граничные маршрутизаторы областей (ABR[1]) G и J будут распространять префикс и SID в магистральную (опорную — backbone) область путем создания нового экземпляра префикса в соответствии с обычными правилами распространения между областями IGP.

Узлы C и I будут вести себя одинаково при утечке префиксов из магистральной области в область 1. Поэтому узел S будет видеть префикс 2001:DB8::2:1/128 с Prefix-SID 150, анонсируемый узлами C и I.

Следовательно, в результате Prefix-SID останется присоединенным к связанному с ним префиксу IGP через межобластной процесс, который работает в одном домене SR.

Когда узел S передает трафик по адресу 2001:DB8::2:1/128, он вталкивает Node-SID(150) в качестве активного сегмента и пересылает пакеты узлы A.

Когда пакет прибывает в ABR I (или C), ABR пересылает его в соответствии с активным сегментом Node-SID(150). Пересылка происходит через границы областей с использованием одного и того же Node-SID(150), пока пакет не попадет к получателю.

4. Сегменты BGP

Сегменты BGP могут назначаться и распространяться протоколом BGP.

4.1. Сегмент BGP-Prefix

Сегмент BGP-Prefix является сегментом BGP, присоединенным к префиксу BGP.

Сегмент BGP-Prefix является глобальным (если явно не анонсируется иное) внутри домена SR.

Сегмент BGP-Prefix в BGP является эквивалентом сегмента IGP-Prefix.

Вероятным применением сегментов BGP-Prefix является крупномасштабная «скелетообразная» топология (hyper-scale spine-leaf) без IGP, где информация о связности получается исключительно от протокола BGP [RFC7938].

4.2. Сегменты партнерства BGP

В контексте BGP EPE[2], как описано в [SR-CENTRAL-EPE], поддерживающий EPE выходной узел **может** анонсировать сегменты, соответствующие его подключенным партнерам. Эти сегменты называются сегментами партнерства BGP или BGP peering SID. Они позволяют выражать заданные отправителем пути между доменами.

Входной граничный маршрутизатор автономной системы (AS[3]) может создать список сегментов для направления потока по выбранному пути внутри AS в направлении выбранного выходного граничного маршрутизатора C данной AS через конкретного партнера. Правила организации партнерства BGP, применяемые на входном узле, включают как минимум два сегмента - Node-SID выбранного выходного узла и сегмент партнерства BGP для выбранного выходного партнера или партнерского интерфейса.

Определены три типа сегментов партнерства BGP - PeerNode SID, PeerAdj SID и PeerSet SID.

- PeerNode SID является локальным сегментом, на анонсирующем его узле BGP семантика сегмента включает:
  - операция SR: NEXT.
  - Next-Hop: подключенный партнерский узел, к которому относится сегмент.
- PeerAdj SID является локальным сегментом, на анонсирующем его узле BGP семантика сегмента включает:
  - операция SR: NEXT.
  - Next-Hop: партнер, подключенный через интерфейс, с которым связан сегмент.
- PeerSet SID является локальным сегментом, на анонсирующем его узле BGP семантика сегмента включает:
  - операция SR: NEXT.
  - Next-Hop: балансировка нагрузки через любой подключенный интерфейс к любому партнеру в связанной группе.

  Набор партнеров может включать всех подключенных партнеров из той же AS или их подмножество. Группа может охватывать несколько AS. Определение группы является правилом, задаваемым оператором.

Расширения BGP, требуемые для сигнализации этих сегментов партнерства BGP, определены в [BGPLS-SR-EPE].

[1]Area Border Router.
[2]Egress Peer Engineering — организация исходящих партнеров.
[3]Autonomous System.

5. Сегмент привязки

Для обеспечения масштабируемости, затенения сетей и независимости служб в SR используется Binding SID (BSID). BSID связан с политикой SR Policy, экземпляр которой может включать список SID. Любые пакеты, принятые с активным сегментом, совпадающим с BSID, управляются привязанной SR Policy.

BSID может представлять собой локальный или глобальный идентификатор SID. Локальные BSID **следует** выделять из SRLB, глобальные **должны** выделяться из SRGB.

Использование BSID позволяет сохранять экземпляр политики (список SID) лишь на узлах, которым требуется наложить политику. Направление трафика узлу, поддерживающему политику, требует только наложения BSID. Если политика меняется, это означает, что менять потребуется лишь узлы, на которые наложена эта политика. На пользователей политики воздействия не оказывается.

5.1. Сегмент IGP Mirroring Context

Одним из вариантов использования сегмента привязки является поддержка для узла IGP анонсирования его способности обрабатывать трафик, исходно адресованный другому узлу IGP (отраженный узел), указанному адресом IP или Node-SID, при условии, что сегмент контекста отражения (Mirroring Context) вставляется в список сегментов до любого сегмента сервиса, который является локальным на отраженном узле.

Когда данный узел B хочет обеспечить защиту выходного узла A, он анонсирует сегмент, указывающий контекст узла A. Такой сегмент называют сегментом контекста отражения и он указывается идентификатором Mirror SID.

Mirror SID анонсируется с использованием сегмента привязки, определенного в расширениях SR IGP [ISIS-SR-EXT].

В случае отказа точка локального ремонта (PLR[1]), перенаправляющая трафик с A на B, вталкивает (PUSH) Mirror SID для защищенного трафика. При получении трафика с Mirror SID в качестве активного сегмента B использует этот сегмент и обрабатывает нижележащие сегменты в контексте A.

6. Групповая адресация

Маршрутизация по сегментам определена для индивидуального трафика и ее расширение на область групповой пересылки выходит за рамки этого документа.

7. Взаимодействие с IANA

Документ не требует действий сос тороны IANA.

8. Вопросы безопасности

Маршрутизацию по сегментам можно применять для уровней данных MPLS и IPv6.

SR добавляет к пакету метаданные (инструкции) со списком элементов пути пересылки (например, узлов, каналов, служб и т. п.), через которые пакет должен пройти. Отмечено, что полный путь заданной отправителем маршрутизации может быть представлен одним сегментом. Это сегмент привязки - Binding SID.

По умолчанию SR работает внутри доверенного домена. Трафик **должен** фильтроваться на границе домена.

Важное значение имеет использование накопленного опыта для снижения риска несанкционированного доступа внутри доверенного домена. Такой опыт рассмотрен в [RFC4381] и применим как для SR-MPLS, так и для SRv6.

8.1. SR-MPLS

При использовании с уровнем данных MPLS SR не задает нового поведения и не меняет способ работы уровня данных MPLS. Поэтому с точки зрения безопасности этот документ не определяет новых механизмов на уровне данных MPLS.

SR позволяет выражать заданный отправителем путь в виде одного сегмента (Binding SID). По сравнению с RSVP-TE, где также обеспечивается возможность явной маршрутизации, нет основополагающих различий в плане предоставляемой информации. Как RSVP-TE, так и SR позволяют выразить заданный отправителем путь в одном сегменте.

Когда путь задается с использованием одной метки, синтаксис метаданных RSVP-TE [RFC3209] и SR эквивалентен.

Когда заданный отправителем путь выражается списком сегментов, к пакету добавляются метаданные, содержащие заданный отправителем путь, по которому должен пройти пакет, в форме списка сегментов.

Когда путь выражается с использованием стека меток, наличие у кого-либо доступа к смыслу меток (т. е., FEC[2]) означает знание явного пути. Для уровня данных MPLS изменение уровня данных не требуется и не происходит существенного изменения возможности. Тем не менее, использование стека меток будет расширяться.

Маршрутизаторы на границе домена SR **должны** фильтровать любой внешний трафик, направленный по меткам, связанным с сегментом внутри доверенного домена. Это включает метки в SRGB доверенного домена, метки в SRLB конкретного граничного маршрутизатора, а также метки, не входящие ни в один из этих блоков. Внешним считается любой трафик, полученный с интерфейса, подключенного к узлу, находящемуся за пределами доверенного домена.

С точки зрения защиты сети предполагается модель доверия, в которой любой узел, налагающий стек меток, предполагается правомочным для такой операции. Это существенно отличается от обычной практики IP с маршрутизацией по кратчайшему пути, но не имее6т принципиальных отличий от существующих методов явной маршрутизации типа RSVP-TE. По умолчанию для явной маршрутной информации **недопустима** утечка через границу административного домена. Расширения SR, определенные для различных протоколов, используют механизмы защиты этих протоколов типа шифрования, проверки подлинности, фильтрации и т. п.

[1]Point of Local Repair.
[2]Forwarding Equivalence Class — класс эквивалентности пересылки.

В общем случае маршрутизатор с поддержкой SR воспринимает и устанавливает метки только в том случае, когда они были предварительно анонсированы доверенным источником. Полученная информация проверяется с использованием имеющихся протоколов уровня управления, обеспечивающих механизмы защиты и проверки подлинности. SR не определяет дополнительных механизмов защиты к существующим протоколам уровня управления.

SR не вносит сигнализации между источником и промежуточными точками пути. При использовании SR заданный отправителем путь рассчитывается с помощью идентификаторов SID, анонсированных ранее на уровень управления IP. Поэтому в дополнение к фильтрации и контролируемым анонсам SID на границе домена SR требуется фильтрация на уровне данных. Фильтрация **должна** выполняться на уровне пересылки на границе домена SR и может требовать просмотра множества меток (инструкций).

Для уровня данных MPLS не предъявляется новых требований к имеющейся архитектуре, поскольку в MPLS уже разрешена заданная отправителем маршрутизация и создание стеков со множеством меток. А для обеспечения защиты уже используется фильтрация пакетов MPLS на границе области доверия [RFC4381], [RFC5920].

8.2. SRv6

При использовании с уровнем данных IPv6 SR добавляет заголовок SRH [IPv6-SRH] типа Routing Extension, как определено в [RFC8200].

SRH добавляет в пакет IPv6 метаданные со списком элементов пути пересылки (например, узлы, каналы, службы и т. п.), через которые пакет должен пройти, в форме адресов IPv6. Полный путь с заданной отправителем маршрутизацией может быть представлен в пакете с использованием одного сегмента (адреса IPv6).

Граничные маршрутизаторы домена SR **должны** фильтровать любой внешний трафик, направленный по адресам из SRGB доверенного домена или из SRLB конкретного граничного маршрутизатора. Внешним считается любой трафик, полученный с интерфейса, подключенного к узлу, находящемуся за пределами доверенного домена.

С точки зрения защиты сети имеется предполагаемая модель доверия, где каждый узел, добавляющий в пакет SRH, считается имеющим право на такую операцию. Следовательно, по умолчанию **недопустима** утечка явной маршрутной информации через границу административного домена. Расширения SR, определяемые в разных протоколах, используют механизмы защиты этих протоколов типа шифрования, проверки подлинности, фильтрации и т. п.

В общем случае маршрутизатор SRv6 воспринимает и устанавливает идентификаторы сегментов (в форме адресов IPv6) только в том случае, когда SID анонсируются доверенным источником. Полученная информация проверяется с использованием имеющихся протоколов уровня управления, обеспечивающих механизмы защиты и проверки подлинности. SR не определяет дополнительных механизмов защиты к существующим протоколам уровня управления.

Проблемы, которые могут возникать в случаях, когда описанное выше поведение не поддерживается или нарушается предполагаемая модель доверия (например, при взломе защиты), включают:

- злонамеренные маршрутные петли;
- обход контроля доступа;
- сокрытие источника DoS-атаки.

Вопросы безопасности SR при использовании с уровнем данных IPv6 более подробно рассмотрены в [RFC5095]. Новый заголовок IPv6 SRH определен в [IPv6-SRH]. В этом же документе рассматриваются указанные выше проблемы безопасности.

8.3. Контроль перегрузок

SR не вносит новых требований к контролю перегрузок. По умолчанию предполагается доставка трафика в режиме best effort. Контроль перегрузок может быть реализован на оконечных точках. При использовании правил SR распределение пропускной способности может обеспечиваться на основе мониторинга входящего трафика, связанного с сегментом привязки, указывающим SR Policy. Могут применяться и другие решения типа предложенного в [RFC8084].

9. Проблемы управляемости

В сетях с поддержкой SR путь для пакета кодируется в заголовке. Поскольку путь не передается сигнальными протоколами, нужны механизмы OAM для того, чтобы операторы сетей могли проверить эффективность пути, а также отслеживать его жизнеспособность и производительность. Однако следует отметить, что SR позволяет существенно снизить число состояний на транзитных узлах, поэтому снижается и число элементов, которыми должен управлять транзитный узел.

Варианты использования SR OAM для уровня данных MPLS определены в [RFC8403], а процедуры SR OAM для MPLS — в [RFC8287].

Маршрутизаторы SR получают анонсы SID (индексы, метки или адреса IPv6) от разных протоколов маршрутизации, которые расширены для поддержки SR. Каждый из таких протоколов имеет механизмы мониторинга и поиска неполадок, обеспечивающие работу и функции управления для IP-адресов, которые должны быть расширены с целью обеспечения этих функций для SID.

А архитектуре SR используются глобальные сегменты, каждый из которых **должен** быть привязан к уникальному индексу или адресу внутри домена SR. Управление распределением таких индексов и адресов со стороны оператора имеет важную роль в предотвращении неполадок типа ошибочной маршрутизации. В дополнение к правилам и инструментам распределения, имеющимся у операторов, реализациям **следует** защищать сеть в случае обнаружения конфликтов с помощью средств детерминированного устранения конфликтов.

При указании пути в виде стека меток узлам может потребоваться механизм сигнализации уровню управления своих возможностей (размера поддерживаемого стека меток).

Модель данных YANG [RFC6020] для настройки и работы SR определена в [SR-YANG].

При использовании SR с уровнем данных IPv6 сегменты указываются адресами IPv6. Выделение, управление и поиск неполадок для идентификаторов сегментов не отличаются от имеющихся механизмов, применимых к выделению и администрированию адресов IPv6.

Адрес получателя (DA) пакет задает адрес активного сегмента, а список сегментов в SRH — полный путь пакета. Проверка пригодности заданного отправителем пути выполняется путем проверки соответствия DA и SRH в пакете эквивалентным записям в таблице маршрутизации.

В контексте уровня данных SRv6 заданный отправителем путь кодируется в SRH, как описано в [IPv6-SRH]. Заданный отправителем путь SRv6 представляется в заголовке SRH в виде списка адресов IPv6, где активный сегмент указывается в поле DA заголовка IPv6. Обычно при проверке любым узлом заголовка пакета можно вывести путь source-routed, к которому пакет относится. Подобно контексту уровня данных SR-MPLS, реализация может создавать пакеты контроля пути и мониторинга, где путь source-routed помещается в SRH, а каждый сегмент пути помещает в пакет соответствующие данные для сквозного контроля пути и производительности.

10. Литература

10.1. Нормативные документы

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

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, DOI 10.17487/RFC3031, January 2001, <https://www.rfc-editor.org/info/rfc3031>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

10.2. Дополнительная литература

[BGPLS-SR-EPE] Previdi, S., Filsfils, C., Patel, K., Ray, S., and J. Dong, "BGP-LS extensions for Segment Routing BGP Egress Peer Engineering", Work in Progress, draft-ietf-idr-bgpls-segment-routing-epe-15, March 2018.

[IPv6-SRH] Filsfils, C., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, Ed., "IPv6 Segment Routing Header (SRH)", Work in Progress, draft-ietf-6man-segment-routing-header-14, June 2018.

[ISIS-SR-EXT] Previdi, S., Ed., Ginsberg, L., Ed., Filsfils, C., Bashandy, A., Gredler, H., Litkowski, S., Decraene, B., and J. Tantsura, "IS-IS Extensions for Segment Routing", Work in Progress, draft-ietf-isis-segment-routing-extensions-19, July 2018.

[OSPF-SR-EXT] Psenak, P., Previdi, S., Filsfils, C., Gredler, H., Shakir, R., Henderickx, W., and J. Tantsura, "OSPF Extensions for Segment Routing", Work in Progress, draft-ietf-ospf-segment-routing-extensions-25, April 2018.

[OSPFv3-SR-EXT] Psenak, P., Ed., Filsfils, C., Previdi, S., Ed., Gredler, H., Shakir, R., Henderickx, W., and J. Tantsura, "OSPFv3 Extensions for Segment Routing", Work in Progress, draft-ietf-ospf-ospfv3-segment-routing-extensions-13, May 2018.

[PCEP-SR-EXT] Sivabalan, S., Filsfils, C., Tantsura, J., Henderickx, W., and J. Hardwick, "PCEP Extensions for Segment Routing", Work in Progress, draft-ietf-pce-segment-routing-12, June 2018.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, DOI 10.17487/RFC3209, December 2001, <https://www.rfc-editor.org/info/rfc3209>.

[RFC4206] Kompella, K. and Y. Rekhter, "Label Switched Paths (LSP) Hierarchy with Generalized Multi-Protocol Label Switching (GMPLS) Traffic Engineering (TE)", RFC 4206, DOI 10.17487/RFC4206, October 2005, <https://www.rfc-editor.org/info/rfc4206>.

[RFC4381] Behringer, M., "Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4381, DOI 10.17487/RFC4381, February 2006, <https://www.rfc-editor.org/info/rfc4381>.

[RFC4915] Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P. Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC 4915, DOI 10.17487/RFC4915, June 2007, <https://www.rfc-editor.org/info/rfc4915>.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <https://www.rfc-editor.org/info/rfc5095>.

[RFC5120] Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, DOI 10.17487/RFC5120, February 2008, <https://www.rfc-editor.org/info/rfc5120>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/info/rfc5440>.

[RFC5714] Shand, M. and S. Bryant, "IP Fast Reroute Framework", RFC 5714, DOI 10.17487/RFC5714, January 2010, <https://www.rfc-editor.org/info/rfc5714>.

[RFC5920] Fang, L., Ed., "Security Framework for MPLS and GMPLS Networks", RFC 5920, DOI 10.17487/RFC5920, July 2010, <https://www.rfc-editor.org/info/rfc5920>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6549] Lindem, A., Roy, A., and S. Mirtorabi, "OSPFv2 Multi-Instance Extensions", RFC 6549, DOI 10.17487/RFC6549, March 2012, <https://www.rfc-editor.org/info/rfc6549>.

[RFC7938] Lapukhov, P., Premji, A., and J. Mitchell, Ed., "Use of BGP for Routing in Large-Scale Data Centers", RFC 7938, DOI 10.17487/RFC7938, August 2016, <https://www.rfc-editor.org/info/rfc7938>.

[RFC8084] Fairhurst, G., "Network Transport Circuit Breakers", BCP 208, RFC 8084, DOI 10.17487/RFC8084, March 2017, <https://www.rfc-editor.org/info/rfc8084>.

[RFC8202] Ginsberg, L., Previdi, S., and W. Henderickx, "IS-IS Multi-Instance", RFC 8202, DOI 10.17487/RFC8202, June 2017, <https://www.rfc-editor.org/info/rfc8202>.

[RFC8287] Kumar, N., Ed., Pignataro, C., Ed., Swallow, G., Akiya, N., Kini, S., and M. Chen, "Label Switched Path (LSP) Ping/Traceroute for Segment Routing (SR) IGP-Prefix and IGP-Adjacency Segment Identifiers (SIDs) with MPLS Data Planes", RFC 8287, DOI 10.17487/RFC8287, December 2017, <https://www.rfc-editor.org/info/rfc8287>.

[RFC8355] Filsfils, C., Ed., Previdi, S., Ed., Decraene, B., and R. Shakir, "Resiliency Use Cases in Source Packet Routing in Networking (SPRING) Networks", RFC 8355, DOI 10.17487/RFC8355, March 2018, <https://www.rfc-editor.org/info/rfc8355>.

[RFC8403] Geib, R., Ed., Filsfils, C., Pignataro, C., Ed., and N. Kumar, "A Scalable and Topology-Aware MPLS Data-Plane Monitoring System", RFC 8403, DOI 10.17487/RFC8403, July 2018, <http://www.rfc-editor.org/info/rfc8403>.

[SR-CENTRAL-EPE] Filsfils, C., Previdi, S., Dawra, G., Aries, E., and D. Afanasiev, "Segment Routing Centralized BGP Egress Peer Engineering", Work in Progress, draft-ietf-spring-segment-routing-central-epe-10, December 2017.

[SR-MPLS] Bashandy, A., Ed., Filsfils, C., Ed., Previdi, S., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing with MPLS data plane", Work in Progress, draft-ietf-spring-segment-routing-mpls-14, June 2018.

[SR-YANG] Litkowski, S., Qu, Y., Sarkar, P., and J. Tantsura, "YANG Data Model for Segment Routing", Work in Progress, draft-ietf-spring-sr-yang-09, June 2018.

Благодарности

Спасибо Dave Ward, Peter Psenak, Dan Frost, Stewart Bryant, Pierre Francois, Thomas Telkamp, Ruediger Geib, Hannes Gredler, Pushpasis Sarkar, Eric Rosen, Chris Bowers и Alvaro Retana за их комментарии и рецензирование документа.

Участники работы

Перечисленные ниже лица внесли существенный вклад в определение архитектуры сегментной маршрутизации и редактирование этого документа.

Ahmed Bashandy

Cisco Systems, Inc.

Email: bashandy@cisco.com

Martin Horneffer

Deutsche Telekom

Email: Martin.Horneffer@telekom.de

Wim Henderickx

Nokia

Email: wim.henderickx@nokia.com

Jeff Tantsura

Email: jefftant@gmail.com

Edward Crabbe

Email: edward.crabbe@gmail.com

Igor Milojevic

Email: milojevicigor@gmail.com

Saku Ytti

TDC

Email: saku@ytti.fi

Адреса авторов

Clarence Filsfils (редактор)

Cisco Systems, Inc.

Brussels

Belgium

Email: cfilsfil@cisco.com

Stefano Previdi (редактор)

Cisco Systems, Inc.

Italy

Email: stefano@previdi.net

Les Ginsberg

Cisco Systems, Inc.

Email: ginsberg@cisco.com

Bruno Decraene

Orange

FR

Email: bruno.decraene@orange.com

Stephane Litkowski

Orange

France

Email: stephane.litkowski@orange.com

Rob Shakir

Google, Inc.

1600 Amphitheatre Parkway

Mountain View, CA 94043

United States of America

Email: robjs@google.com

Перевод на русский язык

Николай Малых

nmalykh@gmail.com