Internet Engineering Task Force (IETF)
Request for Comments: 9067
Category: Standards Track
ISSN: 2070-1721

Y. Qu
Futurewei
J. Tantsura
Microsoft
A. Lindem
Cisco
X. Liu
Volta Networks
October 2021

A YANG Data Model for Routing Policy

Модель данных YANG для политики маршрутизации

Аннотация

Этот документ определяет модель данных YANG для настройки и управления политикой маршрутизации независимо от его производителя (vendor-neutral). Модель обеспечивает базовую схему политики маршрутизации, которую можно расширить для конкретных протоколов маршрутизации с использованием механизма YANG augment.

Статус документа

Документ относится к категории Internet Standards Track.

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

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9067.

Авторские права

Авторские права (Copyright (c) 2021) принадлежат IETF Trust и лицам, указанным в качестве 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....2
   1.1. Цели и подход....2
2. Терминология и обозначения....2
   2.1. Диаграммы деревьев....2
   2.2. Префиксы в именах узлов данных....3
3. Обзор модели....3
4. Выражение политики маршрута....3
   4.1. Наборы для сопоставления....3
   4.2. Условия политики....4
   4.3. Действия политики....4
   4.4. Вложенные правила....4
5. Исполнение политики....5
6. Применение политики маршрутизации....5
7. Модуль и дерево YANG....5
   7.1. Дерево модели политики маршрутизации....5
   7.2. Модель политики маршрутизации....6
8. Вопросы безопасности....16
9. Взаимодействие с IANA....17
10. Литература....17
   10.1. Нормативные документы....17
   10.2. Дополнительная литература....18
Приложение A. Зависимые от протокола маршрутизации правила....18
Приложение B. Примеры политики....19
Благодарности....20
Адреса авторов....21

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

1. Введение

Документ описывает модель данных YANG [RFC7950] для настройки политики маршрутизации на основе опыта работы сетей различных сервис-провайдеров. Модель не привязана к оборудованию, чтобы позволить операторам управлять конфигурацией политики в средах с маршрутизаторами разных производителей.

Модули YANG в документе соответствуют архитектуре хранилищ данных управления (NMDA) [RFC8342].

1.1. Цели и подход

Модель не претендует на функциональную полноту, она является подмножеством параметров конфигурации политики, доступных в реализациях разных производителей, но поддерживает широко используемые конструкции для управления импортом, экспортом и изменением маршрутов в разных протоколах маршрутизации. Подход к разработке модели заключался в изучении фактических конфигураций политики, применяемых в сетях нескольких операторов, и основное внимание уделено обеспечению возможностей и структуре настройки конфигурации политики, получивших широкое распространение.

Несмотря на различие в деталях выражения политики в средах разных производителей, модель отражает наблюдение, что относительно простой подход «условие-действие» легко сопоставить с несколькими имеющимися реализациями производителей, а также даёт операторам знакомый и прямой способ выражения политики. Побочным эффектом этого подхода является исключение других методов из рассмотрения.

В соответствии с целью создания нейтральной к производителям модели данных в неё включены лишь выражения политики, которые считаются доступными в широко распространённых реализациях. Элементы конфигурации, доступные лишь в одной реализации, не включены в модель в надежде, что они станут доступны в фирменных модулях производителей, дополняющих эту модель.

2. Терминология и обозначения

Ключевые слова **должно** (MUST), **недопустимо** (MUST NOT), **требуется** (REQUIRED), **нужно** (SHALL), **не следует** (SHALL NOT), **следует** (SHOULD), **не нужно** (SHOULD NOT), **рекомендуется** (RECOMMENDED), **не рекомендуется** (NOT RECOMMENDED), **возможно** (MAY), **необязательно** (OPTIONAL) в данном документе интерпретируются в соответствии с BCP 14 [RFC2119] [RFC8174] тогда и только тогда, когда они выделены шрифтом, как показано здесь.

Routing policy - политика маршрутизации
: Политика маршрутизации определяет импорт, экспорт, изменение и анонсирование между экземплярами протоколов маршрутизации или в одном экземпляре протокола.

Policy chain - цепочка политики
: Последовательность определений политики. На цепочку могут указывать ссылки из другого контекста.

Policy statement - оператор политики
: Оператор политики состоит из набора условий и действий (любое из них может быть пустым).

Ниже перечислены термины, определённые в [RFC8342]:

- client - клиент;
- server - сервер;
- configuration - конфигурация;
- system state - состояние системы;
- operational state - рабочее состояние;
- intended configuration - предполагаемая конфигурация.

Ряд терминов определён в [RFC7950]:

- action - действие;
- augment - дополнение;
- container - контейнер;
- container with presence - контейнер присутствия;
- data model - модель данных;
- data node - узел данных;
- feature - свойство, функция;
- leaf - лист;
- list - список;
- mandatory node - обязательный узел;
- module - модуль;
- schema tree - дерево схемы;
- RPC (Remote Procedure Call) operation - вызов удалённой процедуры.

2.1. Диаграммы деревьев

Диаграммы деревьев в этом документе используют обозначения, заданные в [RFC8340].

2.2. Префиксы в именах узлов данных

В этом документе имена узлов данных, действий и других объектов модели данных используются без префиксов, если из контекста очевидно, в каком модуле YANG они определены. В остальных случаях имена указываются со стандартным префиксом соответствующего модуля YANG (Таблица 1).

Таблица 1. Префиксы и соответствующие модули YANG.

Префикс	*Модуль YANG*	*Документ*
if	ietf-interfaces	[RFC8343]
rt	ietf-routing	[RFC8349]
yang	ietf-yang-types	[RFC6991]
inet	ietf-inet-types	[RFC6991]

3. Обзор модели

Модуль политики маршрутизации состоит из 3 частей, кратко описанных ниже.

- Общая схема выражения политики как набора связанных условий и действий, включающего наборы сопоставлений и действий, полезные для разных протоколов маршрутизации.
- Структура, позволяющая протоколам маршрутизации добавлять свои условия и действия с помощью дополнений YANG (augment). Имеется пример для протокола BGP [RFC4271] в нейтральной по отношению к производителям модели данных BGP [IDR-BGP-MODEL]. В Приложении A приведён пример расширения для политики BGP. Приложение не является нормативным, поскольку модель для BGP ещё не завершена.
- Пригодная для многократного применения группировка для присоединения правил импорта и экспорта в контексте настройки маршрутизации для разных протоколов, экземпляров виртуальной маршрутизации и пересылки (Virtual Routing and Forwarding или VRF) и т. п. Это также позволяет создавать цепочки политики и выражать принятое по умолчанию поведение политики. В этом документе цепочки и последовательности политики - это последовательности определений, применяемые в определённом порядке (см. раздел 4).

В модуле используются стандартные типы Internet, такие как адреса IP, номера автономных систем и т. п., определённые в RFC 6991 [RFC6991].

4. Выражение политики маршрута

Политика выражается последовательностью определений верхнего уровня, каждое из которых является последовательностью операторов политики. Операторы состоят из простых кортежей «условие-действие». Условия могут включать несколько операторов сопоставления или сравнения, а действия - набор изменений атрибутов маршрута или указание финального восприятия или отклонения маршрута. Структура показана на рисунке.

```
+--rw routing-policy
   +--rw policy-definitions
      +--ro match-modified-attributes?   boolean
      +--rw policy-definition* [name]
         +--rw name          string
         +--rw statements
            +--rw statement* [name]
               +--rw name          string
               +--rw conditions
               |     ...
               +--rw actions
                     ...
```

4.1. Наборы для сопоставления

Модель представляет коллекцию базовых наборов, которые могут применяться в условиях политики для сопоставлений. Эти наборы подходят для выбора маршрутов из разных протоколов маршрутизации. Их можно дополнить связанными с протоколами моделями, имеющими свои наборы. Заданные наборы показаны ниже.

prefix sets - наборы префиксов

Каждый набор определяет множество префиксов IP с диапазоном или точным значением маски сети.

neighbor sets - наборы соседей

Набор соседних узлов с их адресами IP. Этот набор служит для выбора маршрутов по анонсирующих их соседям.

tag sets - наборы тегов

Каждый набор задаёт базовые значения тегов, которые могут применяться для сопоставления при выборе маршрутов.

Структура модели для заданных наборов показана ниже.

```
+--rw routing-policy
   +--rw defined-sets
   |  +--rw prefix-sets
   |  |  +--rw prefix-set* [name]
   |  |     +--rw name        string
   |  |     +--rw mode?       enumeration
   |  |     +--rw prefixes
   |  |        +--rw prefix-list* [ip-prefix mask-length-lower
   |  |                            mask-length-upper]
   |  |           +--rw ip-prefix           inet:ip-prefix
   |  |           +--rw mask-length-lower    uint8
   |  |           +--rw mask-length-upper    uint8
   |  +--rw neighbor-sets
   |  |  +--rw neighbor-set* [name]
   |  |     +--rw name       string
   |  |     +--rw address*   inet:ip-address
   |  +--rw tag-sets
```

```
          |     +--rw tag-set* [name]
          |        +--rw name         string
          |        +--rw tag-value*   tag-type
```

4.2. Условия политики

Операторы политики состоят из набора условий и действий (любой из них может быть пустым). Условия задают сопоставление атрибутов маршрута с заданным набором (например, набором префиксов) или сравнение с конкретным значением. Сопоставление можно изменить с помощью опций (match-set-options):

all
значение true возвращается при соответствии всех элементов набора;

any
значение true возвращается при соответствии любого элементов набора;

invert
значение true возвращается, если ни один элемент набора не соответствует.

Не все опции подходят для сопоставления с каждым определенным набором (например, сопоставление all не имеет смысла для набора префиксов). Когда это приемлемо, в модели применяется ограниченный набор опций соответствия.

В сравнениях также могут применяться эти опции, например для равенства или неравенства.

Хотя большинство условий политики будут добавлять отдельные модели для протоколов маршрутизации путём дополнений, эта модель политики маршрутизации включает несколько базовых сопоставлений и возможность проверить, какой из протоколов или механизмов установил маршрут (например, BGP, IGP, статика и пр.). Включённые в модель условия показаны ниже.

```
+--rw routing-policy
   +--rw policy-definitions
      +--rw policy-definition* [name]
         +--rw name          string
         +--rw statements
            +--rw statement* [name]
               +--rw conditions
               |  +--rw call-policy?
               |  +--rw source-protocol?
               |  +--rw match-interface
               |  |  +--rw interface?
               |  +--rw match-prefix-set
               |  |  +--rw prefix-set?
               |  |  +--rw match-set-options?
               |  +--rw match-neighbor-set
               |  |  +--rw neighbor-set?
               |  +--rw match-tag-set
               |  |  +--rw tag-set?
               |  |  +--rw match-set-options?
               |  +--rw match-route-type
               |     +--rw route-type*
```

4.3. Действия политики

Когда условия политики выполнены, применяются действия правила для установки различных атрибутов устанавливаемого маршрута или указания финального решения (воспринять или отвергнуть).

Подобно условиям, действия модели политики маршрутизации включают базовые операции в дополнение к финальному решению для маршрута. Эти действия показаны ниже.

```
+--rw routing-policy
   +--rw policy-definitions
      +--rw policy-definition* [name]
         +--rw statements
            +--rw statement* [name]
               +--rw actions
                  +--rw policy-result?   policy-result-type
                  +--rw set-metric
                  |  +--rw metric-modification?
                  |  |         metric-modification-type
                  |  +--rw metric?                 uint32
                  +--rw set-metric-type
                  |  +--rw metric-type?   identityref
                  +--rw set-route-level
                  |  +--rw route-level?   identityref
                  +--rw set-route-preference?      uint16
                  +--rw set-tag?               tag-type
                  +--rw set-application-tag?   tag-type
```

4.4. Вложенные правила

Поддерживаются «подпрограммы» политики (вложенные правила), позволяющие задавать условные ссылки на другие определения с использованием конфигурации вызова правил (call-policy). Вызванные правила применяют свои условия и действия до возврата в вызвавший оператор, после чего продолжается оценка (исполнение) политики. Результат вызова влияет на исполнение вызывающего правила. Если вызванное правило приводит к принятию маршрута (accept-route), «подпрограмма» возвращает вызвавшему правилу логическое значение true. Для вызывающей политики это эквивалентно оператору условия с результатом true, поэтому вызывающая сторона продолжает исполнение политики (см. раздел 5). Отметим, что вызываемое правило может менять атрибуты маршрута в своих операторах действий. Действие reject-route возвращает значение false с соответствующим влиянием на вызвавшую политику. При достижении последнего оператора «подпрограммы» применяется принятое по умолчанию финальное действие (т. е. false для reject-route). Поэтому «подпрограмма» не может явно принять или отклонить маршрут, а вместо этого

возвращает логическое значение true для accept-route и false для reject-route. Принятие или отклонение маршрута полностью определяет политика верхнего уровня.

Отметим, что вызываемая политика сама может вызывать другие правила (реализация может ограничивать это). Модель не задаёт глубину вложенности, поскольку она может меняться в реализациях, например, реализация может поддерживать лишь один уровень рекурсии. Как в любой политике политике маршрутизации, следует соблюдать осторожность при вызовах «подпрограмм», чтобы возвращаемое ими значение обеспечивало нужное поведение. Вложенные правила удобны во многих вариантах политики маршрутизации, но создавать правила с глубокой рекурсией (например, больше 2-3) не рекомендуется. Кроме того, реализации **должны** выполнять проверку отсутствия рекурсии между вложенными правилами маршрутизации.

5. Исполнение политики

Исполнение (оценка) каждого определения политики выполняется путём выполнения отдельных операторов в порядке из указания. Когда все условия в операторе политики соблюдены, исполняются соответствующие операторы действий. Если действие включает accept-route или reject-route, выполнение текущего правила прекращается с переходом к следующему правилу. Если в цепочке политики множество правил, последующие правила цепочки в этом случае не исполняются. Цепочки представляют собой последовательности определений правил, (см. раздел 4).

Если условия не соблюдены, происходит переход к следующему оператору политики. Если не выполняется ни одно из условий оператора политики, исполнение текущего определения прекращается с переходом к следующему определению в цепочке. По достижении конца цепочки правил применяется заданное по умолчанию действие (reject-route, если в цепочке явно не задано иное действие).

Использование предварительных атрибутов для проверки условий в операторе политики зависит от принятого реализацией значения листа match-modified-attributes (сопоставление изменённых атрибутов). Если этот лист имеет значение false и действие меняет атрибуты маршрута, эти изменения не учитываются в операторах условий. Если же match-modified-attributes = true и действие меняет зависящие от приложения атрибуты, изменённые значения участвуют в проверке условий.

6. Применение политики маршрутизации

Политика маршрутизации применяется путём определения и присоединения цепочек правил в разных контекстах маршрутизации. Цепочки правил являются последовательностями определений (см. раздел 4), на которые можно указывать из разных контекстов. Например, цепочка правил может быть связана с протоколом маршрутизации и применяться для управления его взаимодействием с протокольными партнёрами или локальной базой маршрутной информации. С цепочкой правил связано направление (импорт или экспорт) по отношению к ссылающемуся на цепочку контексту.

Модель политики маршрутизации определяет группировку применяемых правил, которую можно импортировать и применять в других моделях. Как показано ниже, это даёт возможность определить цепочки правил импорта и экспорта, а также задать используемое по умолчанию решение для маршрута, если цепочка правил не даёт результата.

```
+--rw apply-policy
|  +--rw import-policy*
|  +--rw default-import-policy?   default-policy-type
|  +--rw export-policy*
|  +--rw default-export-policy?   default-policy-type
```

Принятая по умолчанию политика в этой модели задаёт отклонение (reject) маршрута для импорта и экспорта.

7. Модуль и дерево YANG

7.1. Дерево модели политики маршрутизации

Дерево модели политики маршрутизации показано ниже.

```
module: ietf-routing-policy
  +--rw routing-policy
     +--rw defined-sets
     |  +--rw prefix-sets
     |  |  +--rw prefix-set* [name mode]
     |  |     +--rw name        string
     |  |     +--rw mode        enumeration
     |  |     +--rw prefixes
     |  |        +--rw prefix-list* [ip-prefix mask-length-lower
     |  |                            mask-length-upper]
     |  |           +--rw ip-prefix            inet:ip-prefix
     |  |           +--rw mask-length-lower    uint8
     |  |           +--rw mask-length-upper    uint8
     |  +--rw neighbor-sets
     |  |  +--rw neighbor-set* [name]
     |  |     +--rw name       string
     |  |     +--rw address*   inet:ip-address
     |  +--rw tag-sets
     |     +--rw tag-set* [name]
     |        +--rw name         string
     |        +--rw tag-value*   tag-type
     +--rw policy-definitions
        +--ro match-modified-attributes?   boolean
        +--rw policy-definition* [name]
           +--rw name          string
           +--rw statements
              +--rw statement* [name]
```

```
                  +--rw name          string
                  +--rw conditions
                  |  +--rw call-policy?       -> ../../../../../..
                  |                           /policy-definitions
                  |                           /policy-definition/name
                  |  +--rw source-protocol?      identityref
                  |  +--rw match-interface
                  |  |  +--rw interface?      if:interface-ref
                  |  +--rw match-prefix-set
                  |  |  +--rw prefix-set?     -> ../../../../../../..
                  |  |                        /defined-sets
                  |  |                        /prefix-sets
                  |  |                        /prefix-set/name
                  |  |  +--rw match-set-options?
                  |  |                        match-set-options-type
                  |  +--rw match-neighbor-set
                  |  |  +--rw neighbor-set?   -> ../../../../../../..
                  |  |                        /defined-sets
                  |  |                        /neighbor-sets
                  |  |                        /neighbor-set/name
                  |  +--rw match-tag-set
                  |  |  +--rw tag-set?        -> ../../../../../../..
                  |  |                        /defined-sets/tag-sets
                  |  |                        /tag-set/name
                  |  |  +--rw match-set-options?
                  |  |                        match-set-options-type
                  |  +--rw match-route-type
                  |     +--rw route-type*     identityref
                  +--rw actions
                     +--rw policy-result?         policy-result-type
                     +--rw set-metric
                     |  +--rw metric-modification?
                     |                        metric-modification-type
                     |  +--rw metric?                uint32
                     +--rw set-metric-type
                     |  +--rw metric-type?   identityref
                     +--rw set-route-level
                     |  +--rw route-level?   identityref
                     +--rw set-route-preference?        uint16
                     +--rw set-tag?                tag-type
                     +--rw set-application-tag?   tag-type
```

7.2. Модель политики маршрутизации

В тексте документа нет ссылок на упоминаемые в модуле ietf-routing-policy.yang [RFC2328], [RFC3101], [RFC5130], [RFC5302], [RFC6991], [RFC8343].

```
<CODE BEGINS> file "ietf-routing-policy@2021-10-11.yang"
module ietf-routing-policy {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-routing-policy";
  prefix rt-pol;

  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-interfaces {
    prefix if;
    reference
      "RFC 8343: A YANG Data Model for Interface
                 Management";
  }
  import ietf-routing {
    prefix rt;
    reference
      "RFC 8349: A YANG Data Model for Routing
                 Management (NMDA Version)";
  }

  organization
    "IETF RTGWG - Routing Area Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/rtgwg/>
     WG List:  <mailto: rtgwg@ietf.org>

     Editors:  Yingzhen Qu
               <mailto: yingzhen.qu@futurewei.com>
               Jeff Tantsura
               <mailto: jefftant.ietf@gmail.com>
               Acee Lindem
```

```
                <mailto: acee@cisco.com>
                Xufeng Liu
                <mailto: xufeng.liu.ietf@gmail.com>";
  description
    "Этот модуль описывает модель данных YANG для настройки политики
     маршрутизации. Он включает ограниченный набор параметров
     конфигурации, доступных в реализациях разных производителей, но
     поддерживает широко применяемые конструкции для управления
     импортом, экспортом, изменением и анонсированием маршрутов в
     одном или разных экземплярах протоколов маршрутизации. Модуль
     предназначен для использования с модулями настройки протоколов
     маршрутизации, например BGP), определёнными в других моделях.

     Этот модуль YANG соответствует архитектуре хранилищ управления
     сетью (NMDA), определённой в RFC 8342.

     Ключевые слова ДОЛЖНО, НЕДОПУСТИМО, ТРЕБУЕТСЯ, НУЖНО, НЕ НУЖНО,
     СЛЕДУЕТ, НЕ СЛЕДУЕТ, РЕКОМЕНДУЕТСЯ, НЕ РЕКОМЕНДУЕТСЯ, МОЖНО,
     НЕОБЯЗАТЕЛЬНО в этом документе трактуются в соответствии с
     BCP 14 (RFC 2119) (RFC 8174) тогда и только тогда, когда они
     указаны заглавными буквами, как показано здесь.

     Авторские права (Copyright (c) 2021) принадлежат IETF Trust и
     лицам, указанным как авторы. Все права защищены.

     Распространение и применение модуля в исходной или двоичной
     форме с изменениями или без таковых разрешено в соответствии с
     лицензией Simplified BSD License, изложенной в параграфе 4.c
     IETF Trust's Legal Provisions Relating to IETF Documents
     (https://trustee.ietf.org/license-info).

     Эта версия модуля YANG является частью RFC 9067, где правовые
     аспекты приведены более полно.";

  reference
    "RFC 9067: A YANG Data Model for Routing Policy.";

  revision 2021-10-11 {
    description
      "Initial revision.";
    reference
      "RFC 9067: A YANG Data Model for Routing Policy.";
  }

  /* Отождествления */

  identity metric-type {
    description
      "Базовое отождествление для типов метрики маршрутов.";
  }

  identity ospf-type-1-metric {
    base metric-type;
    description
      "Указывает типы внешней метрики OSPF типа 1. Применимо лишь
       к маршрутам OSPF.";
    reference
      "RFC 2328: OSPF Version 2";
  }

  identity ospf-type-2-metric {
    base metric-type;
    description
      "Указывает типы внешней метрики OSPF типа 2. Применимо лишь
       к маршрутам OSPF.";
    reference
      "RFC 2328: OSPF Version 2";
  }

  identity isis-internal-metric {
    base metric-type;
    description
      "Указывает типы внутренней метрики IS-IS. Применимо лишь
       к маршрутам IS-IS.";
    reference
      "RFC 5302: Domain-Wide Prefix Distribution with
       Two-Level IS-IS";
  }

  identity isis-external-metric {
    base metric-type;
    description
      "Указывает типы внешней метрики IS-IS. Применимо лишь
       к маршрутам IS-IS.";
    reference
      "RFC 5302: Domain-Wide Prefix Distribution with
```

```
        Two-Level IS-IS";
    }

    identity route-level {
      description
        "Базовое отождествление для уровня импорта маршрута.";
    }

    identity ospf-normal {
      base route-level;
      description
        "Отождествление импорта OSPF в обычные области. Применяется
         лишь к маршрутам, импортируемым в OSPF.";
      reference
        "RFC 2328: OSPF Version 2";
    }

    identity ospf-nssa-only {
      base route-level;
      description
        "Отождествление импорта в области OSPF Not-So-Stubby (NSSA).
         Применяется лишь к маршрутам, импортируемым в OSPF.";
      reference
        "RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option";
    }

    identity ospf-normal-nssa {
      base route-level;
      description
        "Отождествление импорта в области OSPF и области NSSA.
         Применяется лишь к маршрутам, импортируемым в OSPF.";
      reference
        "RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option";
    }

    identity isis-level-1 {
      base route-level;
      description
        "Отождествление импорта в области IS-IS Level 1. Применяется лишь
         к маршрутам, импортируемым в протокол IS-IS.";
      reference
        "RFC 5302: Domain-Wide Prefix Distribution with
         Two-Level IS-IS";
    }

    identity isis-level-2 {
      base route-level;
      description
        "Отождествление импорта в области IS-IS Level 2. Применяется лишь
         к маршрутам, импортируемым в протокол IS-IS.";
      reference
        "RFC 5302: Domain-Wide Prefix Distribution with
         Two-Level IS-IS";
    }

    identity isis-level-1-2 {
      base route-level;
      description
        "Отождествление импорта в области IS-IS Level 1 и Level 2. Применяется
         лишь к маршрутам, импортируемым в протокол IS-IS.";
      reference
        "RFC 5302: Domain-Wide Prefix Distribution with
         Two-Level IS-IS";
    }

    identity proto-route-type {
      description
        "Базовое отождествление типа маршрута внутри протокола.";
    }

    identity isis-level-1-type {
      base proto-route-type;
      description
        "Отождествление маршрута IS-IS Level 1. Применяется лишь к маршрутам
         IS-IS.";
      reference
        "RFC 5302: Domain-Wide Prefix Distribution with
         Two-Level IS-IS";
    }

    identity isis-level-2-type {
      base proto-route-type;
      description
        "Отождествление маршрута IS-IS Level 2. Применяется лишь к маршрутам
         IS-IS.";
      reference
```

```
      "RFC 5302: Domain-Wide Prefix Distribution with
       Two-Level IS-IS";
  }

  identity ospf-internal-type {
    base proto-route-type;
    description
      "Отождествление маршрута внутри или между областями OSPF.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 2328: OSPF Version 2";
  }

  identity ospf-external-type {
    base proto-route-type;
    description
      "Отождествление внешнего маршрута OSPF типа 1 или 2.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 2328: OSPF Version 2";
  }

  identity ospf-external-t1-type {
    base ospf-external-type;
    description
      "Отождествление внешнего маршрута OSPF типа 1.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 2328: OSPF Version 2";
  }

  identity ospf-external-t2-type {
    base ospf-external-type;
    description
      "Отождествление внешнего маршрута OSPF типа 2.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 2328: OSPF Version 2";
  }

  identity ospf-nssa-type {
    base proto-route-type;
    description
      "Отождествление маршрута OSPF NSSA типа 1 или 2.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option";
  }

  identity ospf-nssa-t1-type {
    base ospf-nssa-type;
    description
      "Отождествление маршрута OSPF NSSA типа 1.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option";
  }

  identity ospf-nssa-t2-type {
    base ospf-nssa-type;
    description
      "Отождествление маршрута OSPF NSSA типа 2.
       Применяется лишь к маршрутам OSPF.";
    reference
      "RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option";
  }

  identity bgp-internal {
    base proto-route-type;
    description
      "Отождествление маршрутов, полученных от внутреннего BGP (IBGP).
       Применяется лишь к маршрутам BGP.";
    reference
      "RFC 4271: A Border Gateway Protocol 4 (BGP-4)";
  }

  identity bgp-external {
    base proto-route-type;
    description
      "Отождествление маршрутов, полученных от внешнего BGP (EBGP).
       Применяется лишь к маршрутам BGP.";
    reference
      "RFC 4271: A Border Gateway Protocol 4 (BGP-4)";
  }
```

```
/* Определения типов */

typedef default-policy-type {
  type enumeration {
    enum accept-route {
      description
        "Принятое по умолчанию правило восприятия маршрута.";
    }
    enum reject-route {
      description
        "Принятое по умолчанию правило отклонения маршрута.";
    }
  }
  description
    "Тип служит для указания финального решения по маршруту
     в цепочке правил. Применяется в принятых по умолчанию
     правилах импорта и экспорта.";
}

typedef policy-result-type {
  type enumeration {
    enum accept-route {
      description
        "Правило для восприятия маршрута.";
    }
    enum reject-route {
      description
        "Правило для отклонения маршрута.";
    }
  }
  description
    "Тип служит для указания финального решения по маршруту
     в цепочке правил.";
}

typedef tag-type {
  type union {
    type uint32;
    type yang:hex-string;
  }
  description
    "Тип для выражения тегов маршрутов в локальной системе,
     включая IS-IS и OSPF. Может быть десятичным или
     шестнадцатеричным целым числом.";
  reference
    "RFC 2328: OSPF Version 2
     RFC 5130: A Policy Control Mechanism in IS-IS Using
               Administrative Tags";
}

typedef match-set-options-type {
  type enumeration {
    enum any {
      description
        "Имеет значение true, если заданное значение совпадает
         с любым элементом определённого множества.";
    }
    enum all {
      description
        "Имеет значение true, если заданное значение совпадает
         со всеми элементами определённого множества.";
    }
    enum invert {
      description
        "Имеет значение true, если заданное значение не совпадает
         ни с одним элементом определённого множества.";
    }
  }
  default "any";
  description
    "Опции, управляющие поведением оператора match. По умолчанию
     принято any, т. е. совпадение с любым элементом множества.";
}

typedef metric-modification-type {
  type enumeration {
    enum set-metric {
      description
        "Устанавливает конкретное значение метрики.";
    }
    enum add-metric {
      description
        "Добавляет указанное значение к имеющейся метике. При
         переполнении устанавливается максимальное значение (0xffffffff)";
    }
    enum subtract-metric {
```

```
        description
          "Отнимает указанное значение от имеющейся метики. При
           получении отрицательного результата устанавливается 0.";
      }
    }
    description
      "Тип служит для установки нужного значения метрики.";
  }

  /* Группировки */

  grouping prefix {
    description
      "Конфигурационные данные для определения префиксов.

       Комбинация mask-length-lower и mask-length-upper
       задаёт диапазон размеров масок или одно значение, если
       mask-length-lower и mask-length-upper совпадают.

       Пример: диапазон 192.0.2.0/24 - 192.0.2.0/26 будет
       выражаться как prefix: 192.0.2.0/24,
                      mask-length-lower=24,
                      mask-length-upper=26

       Пример: 192.0.2.0/24 (точное совпадение) будет
       выражаться как prefix: 192.0.2.0/24,
                      mask-length-lower=24,
                      mask-length-upper=24

       Пример: диапазон 2001:DB8::/32 - 2001:DB8::/64 будет
       выражаться как prefix: 2001:DB8::/32,
                      mask-length-lower=32,
                      mask-length-upper=64";
    leaf ip-prefix {
      type inet:ip-prefix;
      mandatory true;
      description
        "Префикс IP, представленный как номер сети IPv6 или IPv4,
         за которым следует размер префикса через символ дробной
         черты. Все элементы prefix-set ДОЛЖНЫ относиться к тому
         же семейству адресов, что и режим prefix-set.";
    }
    leaf mask-length-lower {
      type uint8 {
        range "0..128";
      }
      description
        "Нижняя граница размера маски. НЕДОПУСТИМЫ значения меньше
         размера prefix, заданного в ip-prefix.";
    }
    leaf mask-length-upper {
      type uint8 {
        range "1..128";
      }
      must '../mask-length-upper >= ../mask-length-lower' {
        error-message "The upper bound MUST NOT be less "
                    + "than lower bound.";
      }
      description
        "Верхняя граница размера маски. НЕДОПУСТИМЫ значения меньше
         нижней границы.";
    }
  }

  grouping match-set-options-group {
    description
      "Группировка опций, относящихся к сопоставлению с конкретным
       множеством.";
    leaf match-set-options {
      type match-set-options-type;
      description
        "Необязательный параметр, задающий поведение операции
         сопоставления.";
    }
  }

  grouping match-set-options-restricted-group {
    description
      "Группировка для ограниченного набора модификаторов операции
       сопоставления.";
    leaf match-set-options {
      type match-set-options-type {
        enum any {
          description
            "Имеет значение true, если заданное значение совпадает
             с любым элементом определённого множества.";
```

```
        }
        enum invert {
          description
            "Имеет значение true, если заданное значение не совпадает
             ни с одним элементом определённого множества.";
        }
      }
      description
        "Необязательные параметры, управляющие поведением операции
         сопоставления. Этот лист поддерживает лишь опции
         any и invert, но не поддерживает all.";
    }
  }

  grouping apply-policy-group {
    description
      "Контейнер верхнего уровня для применения политики маршрутизации.
       Группировка предназначена для использования в моделях маршрутизации.";
    container apply-policy {
      description
        "Опорная точка для политики маршрутизации в модели. Правила импорта
         и экспорта применяются к локальной таблице маршрутизации, т. е.
         export (передача) и import (приём) в зависимости от контекста.";
      leaf-list import-policy {
        type leafref {
          path "/rt-pol:routing-policy/rt-pol:policy-definitions/"
              + "rt-pol:policy-definition/rt-pol:name";
          require-instance true;
        }
        ordered-by user;
        description
          "Список имён правил в порядке применения при получении
           распространяемых маршрутов от другого протокола маршрутизации
           или обновлении маршрутизации в текущем контексте, например,
           для текущей группы партнёров, соседа, семейства адресов и т. п.";
      }
      leaf default-import-policy {
        type default-policy-type;
        default "reject-route";
        description
          "Явная установка принятой по умолчанию политики, если не выполнено
           определение в цепочке правил импорта.";
      }
      leaf-list export-policy {
        type leafref {
          path "/rt-pol:routing-policy/rt-pol:policy-definitions/"
              + "rt-pol:policy-definition/rt-pol:name";
          require-instance true;
        }
        ordered-by user;
        description
          "Список имён правил в порядке применения при распространении
           маршрутов от одного протокола маршрутизации к другому или
           передаче маршрутного обновления в текущем контексте, например,
           для текущей группы партнёров, соседа, семейства адресов и т. п.";
      }
      leaf default-export-policy {
        type default-policy-type;
        default "reject-route";
        description
          "Явная установка принятой по умолчанию политики, если не выполнено
           определение в цепочке правил экспорта.";
      }
    }
  }
  container routing-policy {
    description
      "Контейнер верхнего уровня для всей политики маршрутизации.";
    container defined-sets {
      description
        "Предопределённый набор атрибутов, используемых в операторах
         сопоставления.";
      container prefix-sets {
        description
          "Определения данных для списка префиксов IPv4 или IPv6,
           сопоставляемых как часть политики.";
        list prefix-set {
          key "name mode";
          description
            "Список определённых наборов префиксов";
          leaf name {
            type string;
            description
              "Имя набора префиксов, используемое как метка для указания
               набора в условиях сопоставления.";
          }
```

```
          leaf mode {
            type enumeration {
              enum ipv4 {
                description
                  "Набор префиксов IPv4.";
              }
              enum ipv6 {
                description
                  "набор префиксов IPv6.";
              }
            }
            description
              "Указывает режим набора префиксов в части присутствия
               семейств адресов (IPv4 или IPv6). Режим служит
               указанием типа, к которому ДОЛЖНЫ относиться все
               префиксы. Устройство ДОЛЖНО проверять все префиксы и
               отвергать конфигурацию в случае несоответствия.";
          }
          container prefixes {
            description
              "Контейнер для списка префиксов в политике. Поскольку
               для отдельных префиксов нет уникальных действий,
               порядок сопоставления префиксов в prefix-list не
               влияет на результат и определяется реализацией. Данное
               условие prefix-set считается выполненным, если префикс
               на входе соответствует любому из префиксов в prefix-set.";
            list prefix-list {
              key "ip-prefix mask-length-lower mask-length-upper";
              description
                "Список префиксов в prefix set.";
              uses prefix;
            }
          }
        }
      }
      container neighbor-sets {
        description
          "Определение данных для списка соседей IPv4 или IPv6,
           которые могут сопоставляться в политике маршрутизации.";
        list neighbor-set {
          key "name";
          description
            "Список наборов соседей для применения в правилах.";
          leaf name {
            type string;
            description
              "Имя набора соседей, служащее меткой для указания в
               сопоставлениях.";
          }
          leaf-list address {
            type inet:ip-address;
            description
              "Список адресов IP для набора соседей.";
          }
        }
      }
      container tag-sets {
        description
          "Определение данных для списка тегов, которые могут
           сопоставляться в политике.";
        list tag-set {
          key "name";
          description
            "Список определений набора тегов.";
          leaf name {
            type string;
            description
              "Имя набора тегов, служащее меткой для указания в
               сопоставлениях.";
          }
          leaf-list tag-value {
            type tag-type;
            description
              "Значение элемента набора тегов.";
          }
        }
      }
    }
    container policy-definitions {
      description
        "Внешний контейнер для списка определений верхнего уровня
         в политике.";
      leaf match-modified-attributes {
        type boolean;
        config false;
```

```
        description
          "Логическое значение, задающее сопоставление с фактическими
           атрибутами маршрута или атрибутами, изменёнными
           предшествующими сопоставлению операторами.";
      }
      list policy-definition {
        key "name";
        description
          "Список определений верхнего уровня с уникальными именами
           (ключ). Предполагается, что эти определения будут указываться
           (по имени) в цепочках правил, заданных в операторах импорта
           или экспорта.";
        leaf name {
          type string;
          description
            "Имя определения верхнего уровня, применяемое для ссылки
             на него.";
        }
        container statements {
          description
            "Внешний (включающий) контейнер для операторов политики.";
          list statement {
            key "name";
            ordered-by user;
            description
              "Операторы политики группируют условия и действия внутри
               определения политики. Они выполняются в порядке указания.";
            leaf name {
              type string;
              description
                "Имя оператора политики.";
            }
            container conditions {
              description
                "Условный оператор для текущего оператора политики.";
              leaf call-policy {
                type leafref {
                  path "../../../../../../"
                     + "rt-pol:policy-definitions/"
                     + "rt-pol:policy-definition/rt-pol:name";
                  require-instance true;
                }
                description
                  "Применяет операторы из указанного определения политики
                   и возвращает управление текущему оператору. Вызываемое
                   правило может само вызывать другие правила (реализация
                   может ограничивать это). Это предназначено для поддержки
                   «подпрограмм» политики. Вызываемому правилу СЛЕДУЕТ
                   включать явное или принятое по умолчанию финальное
                   решение для маршрута, возвращающее значение true
                   (accept-route) или false (reject-route). В противном
                   случае поведение может быть неоднозначным. Вызывающему
                   правилу НЕДОПУСТИМО быть вызванным ранее без возврата
                   (т. е. рекурсия не разрешается).";
              }
              leaf source-protocol {
                type identityref {
                  base rt:control-plane-protocol;
                }
                description
                  "Условие для проверки протокола (метода), применяемого для
                   установки маршрута в локальной таблице маршрутизации.";
              }
              container match-interface {
                leaf interface {
                  type if:interface-ref;
                  description
                    "Ссылка на базовый интерфейс.";
                }
                description
                  "Контейнер для условий сопоставления интерфейса.";
              }
              container match-prefix-set {
                leaf prefix-set {
                  type leafref {
                    path "../../../../../../../defined-sets/"
                       + "prefix-sets/prefix-set/name";
                  }
                  description
                    "Ссылка на заданный набор префиксов.";
                }
                uses match-set-options-restricted-group;
                description
                  "Сопоставление указанного набора префиксов в
                   соответствии с логикой листа match-set-options.";
              }
```

```
        container match-neighbor-set {
          leaf neighbor-set {
            type leafref {
              path "../../../../../../../defined-sets/"
                 + "neighbor-sets/neighbor-set/name";
              require-instance true;
            }
            description
              "Ссылка на заданный набор соседей.";
          }
          description
            "Сопоставление с указанным набором соседей.";
        }
        container match-tag-set {
          leaf tag-set {
            type leafref {
              path "../../../../../../../defined-sets/"
                 + "tag-sets/tag-set/name";
              require-instance true;
            }
            description
              "Ссылка на заданный набор тегов.";
          }
          uses match-set-options-group;
          description
            "Сопоставление указанного набора префиксов в
             соответствии с логикой листа match-set-options.";
        }
        container match-route-type {
          description
            "Контейнер, обеспечивающий условие сопоставления
             route-type";
          leaf-list route-type {
            type identityref {
              base proto-route-type;
            }
            description
              "Условие для сопоставления зависящего от протокола
               типа маршрута. Обычно это применяется при импорте
               маршрутов для выбора маршрутов или установки
               зависящих от протокола атрибутов по типу маршрута.";
          }
        }
      }
      container actions {
        description
          "Top-level container for policy action
           statements.";
        leaf policy-result {
          type policy-result-type;
          description
            "Выбор финального решения для маршрута - восприятие
             (accept) или отклонение (reject).";
        }
        container set-metric {
          leaf metric-modification {
            type metric-modification-type;
            description
              "Указывает, как изменить метрику.";
          }
          leaf metric {
            type uint32;
            description
              "Значение метрики для установки, добавления или вычитания.";
          }
          description
            "Установить метрику для маршрута.";
        }
        container set-metric-type {
          leaf metric-type {
            type identityref {
              base metric-type;
            }
            description
              "Тип метрики маршрута.";
          }
          description
            "Установить тип метрики для маршрута.";
        }
        container set-route-level {
          leaf route-level {
            type identityref {
              base route-level;
            }
            description
              "Уровень импорта маршрута.";
```

```
                }
                description
                  "Набор уровней для импорта или экспорта маршрутов.";
              }
              leaf set-route-preference {
                type uint16;
                description
                  "Набор предпочтения для маршрута, называемый также
                   административной дистанцией. Это позволяет выбрать
                   предпочтительный маршрут из числа ведущих к одному
                   префиксу. Меньшее значение более предпочтительно.";
              }
              leaf set-tag {
                type tag-type;
                description
                  "Набор тегов для маршрута.";
              }
              leaf set-application-tag {
                type tag-type;
                description
                  "Устанавливает тег приложения для маршрута. Зависимый
                   от приложения тег может применяться приложениями,
                   которым нужно отличать семантику и/или правила от
                   тега. Например, теги обычно автоматически анонсируются
                   в OSPF AS-External Link State Advertisement (LSA), а
                   зависимые от приложения теги не анонсируются неявно.";
              }
            }
          }
        }
      }
    }
  }
  <CODE ENDS>
```

8. Вопросы безопасности

Заданный этим документом модуль YANG определяет схему для данных, которая обеспечивает доступ по протоколам управления сетью, таким как NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF является защищённый транспорт с обязательной реализацией протокола SSH (Secure Shell) [RFC6242]. Нижним уровнем RESTCONF является протокол HTTPS с обязательной реализацией защищённого транспорта TLS [RFC8446].

Модель управления доступом к конфигурации сети (Network Configuration Access Control Model или NACM) [RFC8341] позволяет разрешить доступ к предопределенным операциям протокола и содержимому лишь отдельным пользователям NETCONF или RESTCONF.

Многие узлы данных в определённом здесь модуле YANG позволяют доступ для записи, создания, удаления (writable/creatable/deletable, т. е. config true, как установлено по умолчанию). Такие узлы могут содержать конфиденциальные сведения или быть уязвимыми в некоторых сетевых средах. Операции записи (например, edit-config) для таких узлов без подобающей защиты могут отрицательно влиять на работу сети. Ниже перечислены субдеревья и узлы данных с указанием возможных уязвимостей.

/routing-policy/defined-sets/prefix-sets

Изменение набора префиксов может привести к DoS-атаке[1]. Злоумышленник может попытаться изменить наборы префиксов для перенаправления или отбрасывания трафика. Перенаправление может быть частью более сложной атаки для сбора конфиденциальной информации или маскировки службы. Кроме того, может быть реализована DoS-атака в плоскости управления с утечкой большого числа маршрутов в домен протокола маршрутизации (например, BGP).

/routing-policy/defined-sets/neighbor-sets

Изменение набора соседей можно использовать для организации DoS-атаки или более сложных атак как при изменении набора префиксов. Например, можно организовать DoS-атаку, меняя соседей, от которых принимаются маршруты.

/routing-policy/defined-sets/tag-sets

Изменение наборов тегов может служить для организации DoS-атак. Маршруты с некоторыми тегами могут перенаправляться или отбрасываться. Воздействие похоже на результат изменения наборов префиксов или соседей. Однако такие атаки могут быть более сложными для обнаружения, поскольку для этого нужно понимать использование политикой маршрутизации тегов маршрутов и их назначение.

/routing-policy/policy-definitions/policy-definition/statements/statement/conditions

Изменение условий можно использовать для организации DoS-атаки и иных типов атак. Атакующий может поменять условие политики и перенаправить или отбросить трафик. Как и изменение наборов префиксов, соседей и тегов, это может быть частью более сложных атак.

/routing-policy/policy-definitions/policy-definition/statements/statement/actions

Изменение действий можно использовать для организации DoS-атаки и иных типов атак с перенаправлением или отбрасыванием трафика. Как и изменение наборов префиксов, соседей и тегов, это может быть частью более сложных атак. Кроме того, могут изменяться атрибуты маршрутов для организации атак второго уровня, которые сложнее обнаружить.

Некоторые из доступных для чтения узлов модуля YANG могут считаться конфиденциальными или уязвимыми в отдельных сетевых средах. Для таких узлов важно контролировать операции чтения (например, get, get-config, notification). Ниже перечислены субдеревья и узлы данных с указанием возможных уязвимостей.

[1]Denial-of-Service - отказ в обслуживании.

/routing-policy/defined-sets/prefix-sets

Данные из этих узлов могут быть использованы для определения локальных префиксов, уязвимых для DoS-атаки.

/routing-policy/defined-sets/neighbor-sets

Данные из этих узлов могут быть использованы для определения локальных узлов, на которые можно организовать DoS-атаку.

/routing-policy/policy-definitions/policy-definition/statements/

Данные из этих узлов можно использовать для организации DoS-атаки на локальный маршрутизатор. Кроме того, правила и входящие в них условия могут считаться «собственностью» (proprietary), из которой можно узнать партнёров, заказчиков и поставщиков. Сами правила могут включать интеллектуальную собственность и раскрытие сведений из них может привести к утрате конкурентных преимуществ.

Конфигурация политики маршрутизации оказывает существенное влияние на работу сети, поэтому другие модели данных YANG, ссылающиеся на политику маршрутизации, также подвержены уязвимостям, связанным с перечисленными выше узлами данных YANG.

9. Взаимодействие с IANA

Агентство IANA зарегистрировало показанный ниже идентификатор URI в субреестре ns реестра IETF XML Registry [RFC3688]:

```
URI:  urn:ietf:params:xml:ns:yang:ietf-routing-policy
Registrant Contact:  The IESG
XML:  N/A; the requested URI is an XML namespace.

IANA has registered the following YANG module in the "YANG Module
Names" subregistry [RFC6020] within the "YANG Parameters" registry:

Name:  ietf-routing-policy
Maintained by IANA?  N
Namespace:  urn:ietf:params:xml:ns:yang:ietf-routing-policy
Prefix:  rt-pol
Reference:  RFC 9067
```

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>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[RFC3101] Murphy, P., "The OSPF Not-So-Stubby Area (NSSA) Option", RFC 3101, DOI 10.17487/RFC3101, January 2003, <https://www.rfc-editor.org/info/rfc3101>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC5130] Previdi, S., Shand, M., Ed., and C. Martin, "A Policy Control Mechanism in IS-IS Using Administrative Tags", RFC 5130, DOI 10.17487/RFC5130, February 2008, <https://www.rfc-editor.org/info/rfc5130>.

[RFC5302] Li, T., Smit, H., and T. Przygienda, "Domain-Wide Prefix Distribution with Two-Level IS-IS", RFC 5302, DOI 10.17487/RFC5302, October 2008, <https://www.rfc-editor.org/info/rfc5302>.

[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>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <https://www.rfc-editor.org/info/rfc6242>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[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>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

[RFC8341] Bierman, A. and M. Bjorklund, "Network Configuration Access Control Model", STD 91, RFC 8341, DOI 10.17487/RFC8341, March 2018, <https://www.rfc-editor.org/info/rfc8341>.

[RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <https://www.rfc-editor.org/info/rfc8342>.

[RFC8343] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 8343, DOI 10.17487/RFC8343, March 2018, <https://www.rfc-editor.org/info/rfc8343>.

[RFC8349] Lhotka, L., Lindem, A., and Y. Qu, "A YANG Data Model for Routing Management (NMDA Version)", RFC 8349, DOI 10.17487/RFC8349, March 2018, <https://www.rfc-editor.org/info/rfc8349>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

10.2. Дополнительная литература

[IDR-BGP-MODEL] Jethanandani, M., Patel, K., Hares, S., and J. Haas, "BGP YANG Model for Service Provider Networks", Work in Progress, Internet-Draft, draft-ietf-idr-bgp-model-09, 28 June 2020, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-bgp-model-09>.

[W3C.REC-xml11] Bray, T., Paoli, J., Sperberg-McQueen, M., Maler, E., Yergeau, F., and J. Cowan, "Extensible Markup Language (XML) 1.1 (Second Edition)", W3C Consortium Recommendation REC-xml11-20060816, 16 August 2006, <https://www.w3.org/TR/2006/REC-xml11-20060816>.

Приложение A. Зависимые от протокола маршрутизации правила

Модели маршрутизации, требующие возможности применять правила, могут дополнять модель политики маршрутизации протоколами или иной специфической настройкой. Модель политики маршрутизации предполагает, что дополнительные наборы, условия и действия могут добавляться другими моделями.

Приведённый ниже пример показывает, как другая модель данных может дополнить описанную модель данных политики маршрутизации. Используются примеры из документа draft-ietf-idr-bgp-model-09 для демонстрации того, как две части могут работать совместно. Пример не является нормативным применительно к [IDR-BGP-MODEL]. Модель аналогичным способом дополняет относящиеся к BGP условия и действия в соответствующих разделах модели политики маршрутизации. В примере префикс XPath bp: указывает импорт из субмодуля ietf-bgp-policy, а префикс XPath bt: - импорт из субмодуля [IDR-BGP-MODEL].

```
module: ietf-routing-policy
  +--rw routing-policy
     +--rw defined-sets
     |  +--rw prefix-sets
     |  |  +--rw prefix-set* [name]
     |  |     +--rw name        string
     |  |     +--rw mode?       enumeration
     |  |     +--rw prefixes
     |  |        +--rw prefix-list* [ip-prefix mask-length-lower
     |  |                            mask-length-upper]
     |  |           +--rw ip-prefix            inet:ip-prefix
     |  |           +--rw mask-length-lower    uint8
     |  |           +--rw mask-length-upper    uint8
     |  +--rw neighbor-sets
     |  |  +--rw neighbor-set* [name]
     |  |     +--rw name       string
     |  |     +--rw address*   inet:ip-address
     |  +--rw tag-sets
     |  |  +--rw tag-set* [name]
     |  |     +--rw name         string
     |  |     +--rw tag-value*   tag-type
     |  +--rw bp:bgp-defined-sets
     |     +--rw bp:community-sets
     |     |  +--rw bp:community-set* [name]
     |     |     +--rw bp:name      string
     |     |     +--rw bp:member*   union
     |     +--rw bp:ext-community-sets
     |     |  +--rw bp:ext-community-set* [name]
     |     |     +--rw bp:name      string
     |     |     +--rw bp:member*   union
     |     +--rw bp:as-path-sets
     |        +--rw bp:as-path-set* [name]
     |           +--rw bp:name      string
     |           +--rw bp:member*   string
     +--rw policy-definitions
        +--ro match-modified-attributes?   boolean
        +--rw policy-definition* [name]
           +--rw name          string
           +--rw statements
              +--rw statement* [name]
                 +--rw name          string
                 +--rw conditions
                 |  +--rw call-policy?
                 |  +--rw source-protocol?          identityref
                 |  +--rw match-interface
                 |  |  +--rw interface?        if:interface-ref
                 |  +--rw match-prefix-set
                 |  |  +--rw prefix-set?       prefix-set/name
                 |  |  +--rw match-set-options?
                 |  |                        match-set-options-type
                 |  +--rw match-neighbor-set
                 |  |  +--rw neighbor-set?
                 |  +--rw match-tag-set
```

```
                  |  |  +--rw tag-set?
                  |  |  +--rw match-set-options?
                  |  |                          match-set-options-type
                  |  +--rw match-route-type
                  |     +--rw route-type*     identityref
                  |  +--rw bp:bgp-conditions
                  |     +--rw bp:med-eq?       uint32
                  |     +--rw bp:origin-eq?    bt:bgp-origin-attr-type
                  |     +--rw bp:next-hop-in*  inet:ip-address-no-zone
                  |     +--rw bp:afi-safi-in*  identityref
                  |     +--rw bp:local-pref-eq?  uint32
                  |     +--rw bp:route-type?     enumeration
                  |     +--rw bp:community-count
                  |     +--rw bp:as-path-length
                  |     +--rw bp:match-community-set
                  |     |  +--rw bp:community-set?
                  |     |  +--rw bp:match-set-options?
                  |     +--rw bp:match-ext-community-set
                  |     |  +--rw bp:ext-community-set?
                  |     |  +--rw bp:match-set-options?
                  |     +--rw bp:match-as-path-set
                  |        +--rw bp:as-path-set?
                  |        +--rw bp:match-set-options?
                  +--rw actions
                     +--rw policy-result?         policy-result-type
                     +--rw set-metric
                     |  +--rw metric-modification?
                     |  +--rw metric?                uint32
                     +--rw set-metric-type
                     |  +--rw metric-type?   identityref
                     +--rw set-route-level
                     |  +--rw route-level?   identityref
                     +--rw set-route-preference?        uint16
                     +--rw set-tag?               tag-type
                     +--rw set-application-tag?   tag-type
                     +--rw bp:bgp-actions
                        +--rw bp:set-route-origin?
                        |                    bt:bgp-origin-attr-type
                        +--rw bp:set-local-pref?   uint32
                        +--rw bp:set-next-hop?     bgp-next-hop-type
                        +--rw bp:set-med?          bgp-set-med-type
                        +--rw bp:set-as-path-prepend
                        |  +--rw bp:repeat-n?   uint8
                        +--rw bp:set-community
                        |  +--rw bp:method?      enumeration
                        |  +--rw bp:options?
                        |  +--rw bp:inline
                        |  |  +--rw bp:communities*   union
                        |  +--rw bp:reference
                        |     +--rw bp:community-set-ref?
                        +--rw bp:set-ext-community
                           +--rw bp:method?      enumeration
                           +--rw bp:options?
                           +--rw bp:inline
                           |  +--rw bp:communities*   union
                           +--rw bp:reference
                              +--rw bp:ext-community-set-ref?
```

Приложение B. Примеры политики

Ниже приведены примеры XML-представления данных конфигурации с использованием моделей политики маршрутизации и BGP для иллюстрации определения и применения политики. Отметим, что язык XML [W3C.REC-xml11] был упрощён для удобочитаемости.

Ниже показано, как можно определить наборы префиксов и тегов. Условие политики заключается в сопоставлении префиксов и тегов, а действие - в восприятии маршрутов при совпадении.

```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <routing-policy
   xmlns="urn:ietf:params:xml:ns:yang:ietf-routing-policy">

      <defined-sets>
        <prefix-sets>
          <prefix-set>
            <name>prefix-set-A</name>
            <mode>ipv4</mode>
            <prefixes>
              <prefix-list>
                <ip-prefix>192.0.2.0/24</ip-prefix>
                <mask-length-lower>24</mask-length-lower>
                <mask-length-upper>32</mask-length-upper>
              </prefix-list>
              <prefix-list>
                <ip-prefix>198.51.100.0/24</ip-prefix>
                <mask-length-lower>24</mask-length-lower>
                <mask-length-upper>32</mask-length-upper>
```

```
                  </prefix-list>
                </prefixes>
              </prefix-set>
              <prefix-set>
                <name>prefix-set-B</name>
                <mode>ipv6</mode>
                  <prefixes>
                  <prefix-list>
                    <ip-prefix>2001:DB8::/32</ip-prefix>
                    <mask-length-lower>32</mask-length-lower>
                    <mask-length-upper>64</mask-length-upper>
                  </prefix-list>
                </prefixes>
              </prefix-set>
            </prefix-sets>
            <tag-sets>
             <tag-set>
              <name>cust-tag1</name>
              <tag-value>10</tag-value>
            </tag-set>
          </tag-sets>
        </defined-sets>

        <policy-definitions>
         <policy-definition>
           <name>export-tagged-BGP</name>
           <statements>
             <statement>
               <name>term-0</name>
               <conditions>
                 <match-prefix-set>
                   <prefix-set>prefix-set-A</prefix-set>
                 </match-prefix-set>
                 <match-tag-set>
                   <tag-set>cust-tag1</tag-set>
                 </match-tag-set>
               </conditions>
               <actions>
                 <policy-result>accept-route</policy-result>
               </actions>
             </statement>
           </statements>
         </policy-definition>
       </policy-definitions>

      </routing-policy>
  </config>
```

В следующем примере все маршруты в RIB получаются из анонсов OSPF, соответствующих внутриобластным и межобластным типам маршрутов OSPF, которые следует передать в анонсы IS-IS уровня 2.

```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <routing-policy
   xmlns="urn:ietf:params:xml:ns:yang:ietf-routing-policy">
   <policy-definitions>
    <policy-definition>
     <name>export-all-OSPF-prefixes-into-IS-IS-level-2</name>
      <statements>
       <statement>
         <name>term-0</name>
         <conditions>
           <match-route-type>
             <route-type>ospf-internal-type</route-type>
           </match-route-type>
         </conditions>
         <actions>
           <set-route-level>
             <route-level>isis-level-2</route-level>
           </set-route-level>
           <policy-result>accept-route</policy-result>
         </actions>
       </statement>
      </statements>
    </policy-definition>
   </policy-definitions>
  </routing-policy>
</config>
```

Благодарности

Определённый в этом документе модуль политики маршрутизации основан на модели политики маршрутизации OpenConfig. Авторы признательны разработчикам OpenConfig за их вклад, особо отмечая Anees Shaikh, Rob Shakir, Kevin D'Souza, Chris Chase.

Авторы благодарны Ebben Aires, Luyuan Fang, Josh George, Stephane Litkowski, Ina Minei, Carl Moberg, Eric Osborne, Steve Padgett, Juergen Schoenwaelder, Jim Uttaro, Russ White, John Heasley за ценный вклад в этот документ и связанные с ним модели.

Спасибо Mahesh Jethanandani, John Scudder, Alvaro Retana, Chris Bowers, Tom Petch, Kris Lambrechts за их рецензии и комментарии.

Адреса авторов

Yingzhen Qu
Futurewei
2330 Central Expressway
Santa Clara, CA 95050
United States of America
Email: yingzhen.qu@futurewei.com

Jeff Tantsura
Microsoft
Email: jefftant.ietf@gmail.com

Acee Lindem
Cisco
301 Midenhall Way
Cary, NC 27513
United States of America
Email: acee@cisco.com

Xufeng Liu
Volta Networks
Email: xufeng.liu.ietf@gmail.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru