

Internet Engineering Task Force (IETF)  
Request for Comments: 8969  
Category: Informational  
ISSN: 2070-1721

Q. Wu, Ed.  
Huawei  
M. Boucadair, Ed.  
Orange  
D. Lopez  
Telefonica I+D  
C. Xie  
China Telecom  
L. Geng  
China Mobile  
January 2021

## A Framework for Automating Service and Network Management with YANG

Модель автоматизации управления сетью и службами с помощью YANG

### Аннотация

Модели данных обеспечивают программируемый подход к представлению служб и сетей. Их можно применять для вывода данных конфигурации компонентов сетей и служб, а также данных состояния для отслеживания и мониторинга. Модели данных могут работать в течение жизненного цикла службы и управления сетью (например, создание экземпляров служб, предоставление, оптимизация, мониторинг, диагностика и гарантированное предоставление услуг). Модели данных играют важную роль в автоматизации управления сетями и могут обеспечивать обратную связь для адаптивного и детерминированного создания, предоставления и поддержки услуг.

В документе описывается модель для автоматизации управления службами и сетью с использованием преимуществ технологии моделирования YANG. Схема организована с точки зрения оператора сети независимо от происхождения модели данных, т. е. может поддерживать модули YANG, созданные вне IETF.

### Статус документа

Документ относится к категории Internet Standards Track.

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

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке <https://www.rfc-editor.org/info/rfc8969>.

### Авторские права

Copyright (c) 2021. Авторские права 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
2. Термины и сокращения.....	3
2.1. Термины.....	3
2.2. Сокращения.....	3
3. Цели и концепции архитектуры.....	4
3.1. Модели данных - уровни и представление.....	4
3.3. Автоматизация предоставления услуг.....	5
3.4. Интеграция с модулем YANG.....	6
4. Функциональные блоки и взаимодействия.....	6
4.1. Процедура управления жизненным циклом службы.....	6
4.1.1. Раскрытие сервиса.....	6
4.1.2. Создание и изменение служб.....	7
4.1.3. Гарантированное обслуживание.....	7
4.1.4. Оптимизация службы.....	7
4.1.5. Диагностика службы.....	7
4.1.6. Прекращение использования услуги.....	7
4.2. Процедура управления предоставлением услуги.....	7
4.2.1. Предоставление предусмотренной конфигурации.....	7
4.2.2. Проверка конфигурации.....	8

<sup>1</sup>Internet Engineering Task Force - комиссия по решению инженерных задач Internet.  
<sup>2</sup>Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

4.2.3. Мониторинг производительности.....	8
4.2.4. Диагностика отказов.....	8
4.3. Многоуровневое и многодоменное представление.....	8
4.4. Декомпозиция службы.....	8
5. Примеры интеграции с моделью данных YANG.....	8
5.1. Предоставление услуг L2VPN/L3VPN.....	8
5.2. Управление жизненным циклом VN.....	9
5.3. Телеметрия по событиям в самоуправлении устройства.....	10
6. Вопросы безопасности.....	10
6.1. Уровень службы.....	11
6.2. Уровень сети.....	11
6.3. Уровень устройства.....	11
7. Взаимодействие с IANA.....	11
8. Литература.....	11
8.1. Нормативные документы.....	11
8.2. Дополнительная литература.....	11
Приложение А. Обзор примеров многоуровневых модулей YANG.....	15
А.1. Модели служб - определения и примеры.....	15
А.2. Монтирование схемы.....	16
А.3. Модели служб - примеры.....	16
А.4. Модели устройств - примеры.....	17
А.4.1. Модели для компоновки.....	17
А.4.2. Управление устройством.....	17
А.4.3. Управление интерфейсом.....	18
А.4.4. Примеры моделей для устройств.....	18
Благодарности.....	19
Участники работы.....	19
Адреса авторов.....	19

## 1. Введение

Системы управления услугами обычно включают активацию и предоставление, а также эксплуатацию служб. Современные процедуры доставки услуг от обработки требований и заказов клиентов до доставки и эксплуатации услуг обычно предполагают последовательное манипулирование данными в нескольких системах поддержки операций (Operations Support System или OSS) или поддержки бизнеса (Business Support System или BSS), которые могут управляться разными подразделениями поставщика услуг (например, отдел счетов, отдел проектирования, центр управления сетью). Многие из таких приложений разрабатываются собственными силами на протяжении многих лет и работают автономно. В результате:

- отсутствуют стандарты ввода-вывода данных (т. е. модель данных), что вызывает проблемы при интеграции и зачастую ведёт к необходимости настройки вручную;
- системы исполнения услуг могут иметь ограниченную видимость состояния сети и поэтому медленно реагировать на изменения в сети.

Программно определяемые сети (Software-Defined Networking или SDN) становятся все более важными для решения этих задач. Методы SDN предназначены для автоматизации общих процедур предоставления услуг и обычно основаны на стандартных моделях данных. Эти модели служат не только для отражения мастерства поставщиков услуг, но и для динамического создания и применения набора определяемых услугами правил, который лучше всего соответствует тому, что было определено и, возможно, согласовано с клиентом. В [RFC7149] представлена предварительная попытка рационализировать точку зрения поставщиков услуг на пространство SDN путём указания конкретных технических областей, которые нужно рассмотреть и для которых могут быть предложены решения.

- Методы динамического обнаружения топологии, устройств и возможностей вместе с соответствующими сведениями и моделями данных, которые предназначены для точного документирования такой топологии, устройств и их возможностей.
- Методы раскрытия сетевых услуг [RFC8309] и их характеристик.
- Методы, применяемые схемами динамического распределения ресурсов и применения правил на основе услуг, чтобы сети можно было программировать должным образом.
- Механизмы динамической обратной связи, предназначенные для оценки применения данной политики (набора правил) с точки зрения предоставления услуг и обеспечения гарантий.

Модели служат ключом для каждого из указанных выше 4 технических элементов. Автоматизация управления службами и сетью является важным шагом к повышению гибкости работы сетей. Модели важны также для интеграции решений разных производителей.

Разработчики YANG [RFC7950] использовали подходы «сверху вниз» и «снизу вверх» для создания модулей [RFC8199] и организации сопоставления между топологией сети и требованиями клиента наверху или абстрагирования базовых конструкций от различных сетевых технологий внизу. На момент подготовки этого документа (2020 г.) было уже много моделей данных YANG, включая модели конфигурации и служб, которые были приняты или рассматривались для принятия IETF. Они охватывают множество протоколов и методов. Однако способы сочетания этих моделей для настройки функций, управления множеством устройств, вовлечённых в службу, или предоставления услуги в настоящее время не документировано ни IETF, ни другими органами стандартизации (Standards Development Organization или SDO).

Многие из указанных в документе модулей YANG применяются для обмена данными между клиентами и серверами NETCONF/RESTCONF [RFC6241][RFC8040]. Тем не менее, YANG является независимым от транспорта языком моделирования данных и может применяться независимо от NETCONF и RESTCONF. Например, YANG можно

применять для задания абстрактных структур данных [RFC8791] которыми могут манипулировать другие протоколы, такие как [DOTS-DDOS].

Этот документ описывает архитектурную модель для автоматизации управления сетью и службами (3. Цели и концепции архитектуры), использующую преимущества технологии моделирования YANG, и исследует взаимодействие между моделями YANG на разных уровнях (например, управление сервисом, компоновка модели) в контексте предоставления услуги (4. Функциональные блоки и взаимодействия). Схема может обеспечить указанные ниже преимущества.

- Независимые от производителей интерфейсы управления службой и базовой сетью.
- Переход от схем внедрения с зависящими от производителя диспетчерами сети к схеме с унифицированными элементами, отвечающими за организацию и управление службами и сетевыми ресурсами на устройствах разных производителей.
- Наследование и многократное применение данных на разных уровнях архитектуры, способствующее предоставлению ресурсов, вместо настройки конфигурации отдельных устройств.
- Динамическое представление процессу принятия решений (например, контроллерам, оркестраторам) уведомлений, инициирующих соответствующие действия, что позволяет этому процессу постоянно подстраивать сеть (и задействованные ресурсы) для предоставления услуг в соответствии с предусмотренными параметрами (целями обслуживания).

Схема представлена с точки зрения оператора сети, независимо от источника данных и позволяет применять модули YANG, разработанные вне IETF. Документ охватывает модели услуг, используемые операторами, для раскрытия своих служб и фиксации требованиям к услугам от клиентов (включая других операторов). Однако в документе не рассматриваются подробно протоколы связи, применяющие эти модели служб для запроса и предоставления услуг.

Документ включает варианты применения для иллюстрации предлагаемого подхода (5. Примеры интеграции с моделью данных YANG), но не претендует на полноту списка таких вариантов. В Приложении А даны некоторые примеры представления многоуровневых модулей YANG.

## 2. Термины и сокращения

### 2.1. Термины

Ниже приведены термины, определённые в [RFC8309] и [RFC8199].

- Network Operator - оператор сети.
- Customer - клиент, заказчик.
- Service - сервис, служба.
- Data Model - модель данных.
- Service Model - модель службы.
- Network Element Model - модель элемента сети.

Этот документ также определяет ряд терминов.

#### **Network Model - модель сети**

Указывает абстракцию сетевого уровня (или подмножество аспектов сетевой инфраструктуры), включая устройства и их подсистемы, а также имеющие отношение к делу протоколы, работающие на канальном и сетевом уровне на нескольких устройствах. Эта модель соответствует модели конфигурации сети из [RFC8309].

Модель может применяться сетевыми операторами для выделения ресурсов (например, туннели, топология) для служб или планирования ресурсов в соответствии с требованиями, заданными в модели сервиса.

#### **Network Domain - сетевой домен**

Указывает разделение сети, которое обычно применяют операторы сетей для разграничения частей своей сети. Примерами доменов могут служить сеть доступа (access network) и ядро сети (core network).

#### **Device Model - модель устройства**

Модель YANG для элемента сети, описанная в [RFC8199], или модель конфигурации устройства, рассмотренная в [RFC8309]. Термин применяется также для моделей функций, встроенных в устройство (например, трансляция адресов (Network Address Translation или NAT) [RFC8512] и списков контроля доступа (Access Control List или ACL) [RFC8519]).

#### **Pipe - канал**

Область взаимодействия 1:1, например, между выходным и входным узлом, двумя сайтами служб и т. п.

#### **Hose - «распылитель»**

Область взаимодействия одного со многими (1:N), например, одного сайта с несколькими.

#### **Funnel - воронка**

Область взаимодействия многих с одним (N:1).

### 2.2. Сокращения

ACL	Access Control List - список управления доступом;
AS	Autonomous System - автономная система;
AP	Access Point - точка доступа;
CE	Customer Edge - граница клиента;
DBE	Data Border Element - граничный элемент данных;
E2E	End-to-End - сквозной;
ECA	Event Condition Action - действие по событию;
L2VPN	Layer 2 Virtual Private Network - виртуальная частная сеть канального уровня;
L3VPN	Layer 3 Virtual Private Network - виртуальная частная сеть сетевого уровня;
L3SM	L3VPN Service Model - модель службы L3VPN;
L3NM	L3VPN Network Model - модель сети L3VPN;
NAT	Network Address Translation - трансляция сетевых адресов;
OAM	Operations, Administration, and Maintenance - операции, администрирование, управление (поддержка);

OWD	One-Way Delay - задержка в одном направлении;
PE	Provider Edge - граница провайдера;
PM	Performance Monitoring - мониторинг производительности;
QoS	Quality of Service - качество обслуживания;
RD	Route Distinguisher - различитель маршрутов;
RT	Route Target - цель маршрута;
SBE	Session Border Element - граничный элемент сессии;
SDN	Software-Defined Networking - программно определяемая сеть;
SP	Service Provider - поставщик услуг;
TE	Traffic Engineering - организация (построение) трафика;
VN	Virtual Network - виртуальная сеть;
VPN	Virtual Private Network - виртуальная частная сеть;
VRF	Virtual Routing and Forwarding - виртуальная маршрутизация и пересылка.

### 3. Цели и концепции архитектуры

#### 3.1. Модели данных - уровни и представление

Как описано в разделе 2 [RFC8199], уровни в моделях улучшают многократное использование модулей нижних уровней модулями более высокого уровня и при этом ограничивают дублирование функций на разных уровнях.

Модели данных в контексте управления сетью можно разделить на модели служб, сетей и устройств. Разные модели услуг могут быть основаны на одних и тех же моделях сетей и/или устройств.

В моделях служб традиционно применяется нисходящий подход и они в основном представляют ориентированные на клиента модули YANG, обеспечивающие общую модельную конструкцию для сетевых служб верхнего уровня (например, L3VPN). Такие модули можно сопоставить со специфичными для сетевых технологий модулями (туннели, маршрутизация, QoS, безопасность). Например, модели служб можно применять для характеристики сетевых услуг, обеспечиваемых между узлами службы (вход-выход), такими как:

- область действия коммуникаций (канал, «распылитель», «воронка и т. п.);
- направленность (входной-выходной);
- гарантии производительности для трафика, выраженные такими показателями, как односторонняя задержка (OWD) [RFC7679] или односторонние потери (One-Way Loss) [RFC7680] (сводку показателей, поддерживаемых IANA, можно найти в [IPPM]);
- пропускная способность канала [RFC5136] [METRIC-METHOD];
- и пр.

На рисунке 1 дан пример голосовой связи по IP (Voice over IP или VoIP), основанной на услугах подключения, предоставляемых оператором сети. Услуги VoIP здесь предоставляются клиентам сетевого оператора сервис-провайдером SP1. Для обеспечения глобальной доступности VoIP, сайт SP1 связан с сайтами других SP, как правило, путём соединения граничных элементов SBE и граничных элементов данных (DBE) [RFC5486][RFC6406]. Для других адресатов VoIP сессии организуются через Internet. Эти услуги связности можно зафиксировать в модели службы YANG, отражающей атрибуты сервиса, показанные на рисунке 2. Этот пример соответствует профилю обеспечения связности IP (IP Connectivity Provisioning Profile), заданному в [RFC7297].

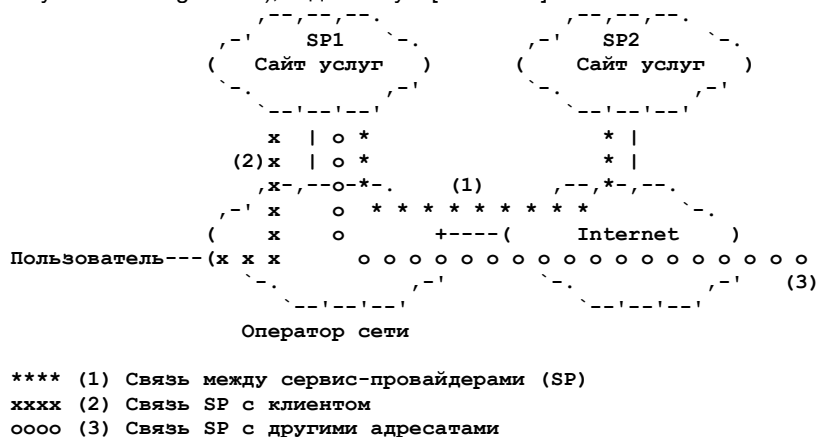


Рисунок 1. Пример компонентов связности служб.

На рисунке 2 «класс с полной гарантией производительности для трафика» указывает класс обслуживания, где гарантируются все показатели производительности трафика, включённые в модель сервиса (OWD, потери, вариации задержки), а «класс с гарантиями задержки для трафика» - класс обслуживания, где гарантируется лишь OWD.

#### Связность - область действия и гарантии

- (1) Связность между SP
  - канал от локального к удалённому SBE/DBE;
  - класс с полной гарантией производительности для трафика.
- (2) Связность между клиентом и SP
  - «распылитель»/«воронка» от локальных SBE/DBE к точкам доступа клиента;
  - класс с полной гарантией производительности для трафика.
- (3) Связность SP с другими адресатами
  - «распылитель»/«воронка» от локальных SBE/DBE к шлюзу Internet;
  - класс с гарантиями задержки для трафика.

**Идентификация потоков**

- IP-адрес получателя (SBE, DBE);
- маркировка DSCP.

**Изоляция трафика**

VPN

**Маршрутизация и пересылка**

Правила маршрутизации для исключения некоторых AS на пути между доменами.

**Уведомления (включая обратную связь)**

- статистика суммарного трафика для настройки пропускной способности;
- отказы;
- плановое обслуживание по порогам.

Рисунок 2. Простые атрибуты, собранные в модель сервиса.

Модели сетей в основном представляют собой модули, обращённые к сетевым ресурсам, и описывают различные аспекты сетевой инфраструктуры, включая устройства и их подсистемы, а также связанные с ними протоколы, работающие на канальном и сетевом уровне на нескольких устройствах (например, сетевую топологию и управление трафиком в туннелях). Модели устройств (и функций) обычно используют восходящий подход и являются в основном связанными с технологией модулями, служащими для реализации услуг (например, BGP, ACL).

Каждый уровень поддерживает представление поддерживаемых модулей YANG, обеспечиваемое нижележащим уровнем (см., например, Приложение А). Могут применяться такие механизмы, как библиотека YANG [RFC8525], для раскрытия модулей YANG, поддерживаемых узлами на нижележащих уровнях.

На рисунке 3 показана модель уровней. Обзор по оркестраторам и контроллерам можно найти в разделе 4 [RFC8309]. За все эти элементы (оркестраторы, контроллеры, устройства) отвечает один оператор.

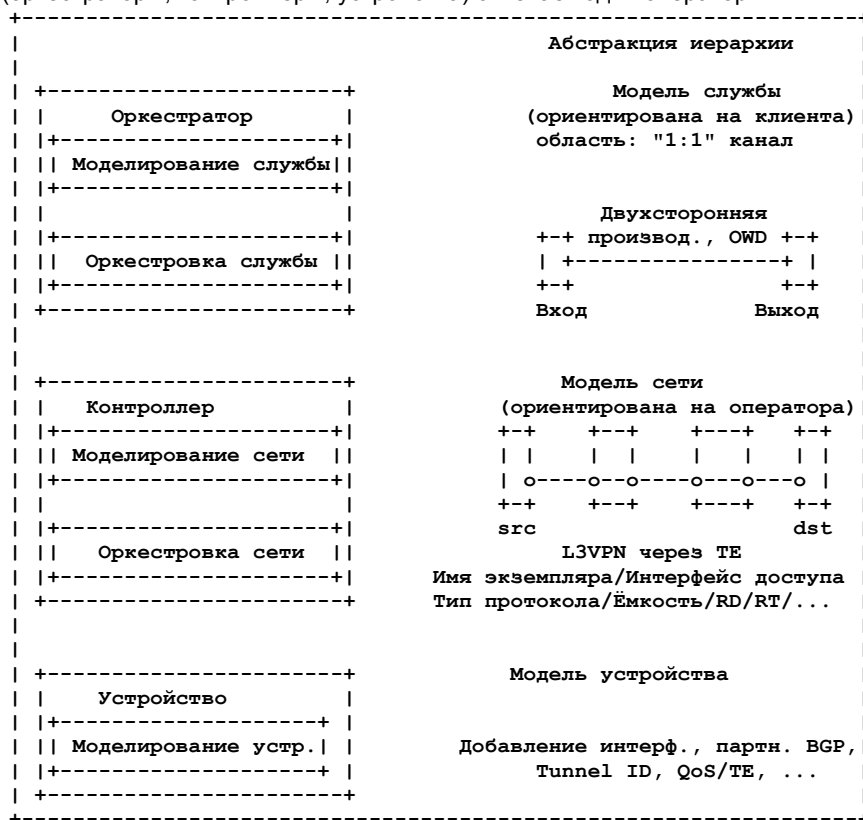


Рисунок 3. Уровни и представление у оператора.

Составная услуга, предоставляемая оператором, может работать на основе услуг других операторов. В таком случае оператор выступает как клиент для запроса услуг других сетей. Операторы, предоставляющие такие услуги, используют уровни, показанные на рисунке 3. Сопоставление составной услуги со сторонними службами поддерживается на уровне оркестровки. С точки зрения плоскости данных соответствующие правила управления трафиком (например, цепочки сервисных функций [RFC7665]) поддерживаются сетевыми контроллерами для указания, как и когда нужно вызывать сторонние службы для потоков, связанных с составной услугой.

Модель уровней на рисунке 3 не делает предположений о местоположении различных объектов (например, контроллера или оркестратора) внутри сети. Поэтому архитектура не исключает развёртывания, например, при встраивании контроллера в устройство, на котором размещены другие функции, контролируемые модулями YANG.

Для упрощения сопоставления между уровнями и многократным использованием данных этот документ уделяет основное внимание моделям служб с использованием YANG. Тем не менее, в полном соответствии с разделом 3 в [RFC8309], рисунок 3 не исключает моделирования служб с использованием языков, отличных от YANG.

### 3.3. Автоматизация предоставления услуг

Для работы службы настройки параметров в моделях устройств выводятся из моделей служб и/или моделей сетей с указанными ниже целями.

- Обеспечение каждого вовлечённого сетевого устройства (функции) соответствующими настройками.
- Работа сети на основе требований службы из моделей служб и локальных инструкций по настройке.

Кроме того, рабочее состояние, включая действующую конфигурацию и статистику, следует раскрывать вышележащим уровням для улучшения видимости сети и оценки соответствия производных модулей нижних уровней входным данным верхних уровней.

К уведомлениям применяются фильтры, которые передаются уровням службы. Тип и частота уведомлений может согласовываться в модели службы.

Отметим, что важно сопоставлять данные телеметрии с данными конфигурации, которые будут применяться для замкнутых контуров на различных этапах доставки услуг от выделения ресурсов до работы службы, в частности.

### 3.4. Интеграция с модулем YANG

Для предоставления услуг «сверху вниз» модули YANG на разных или одном уровне нужно интегрировать для корректной доставки услуг (включая нужную настройку сети). Например, параметры услуги, зафиксированные в моделях службы, нужно разложить в набор параметров конфигурации и уведомлений, которые могут быть связаны с одной или несколькими технологиями, а эти специфичные для технологии параметры нужно сгруппировать для задания зависящих от топологии моделей на уровне устройств или сети. Кроме того, эти связанные с технологией модели устройств или сети могут быть ещё раз объединены с помощью механизма монтирования схемы [RFC8528] для предоставления каждой задействованной функции (устройству) или домену сети поддержки добавленных модулей или функций. Набор интегрированных моделей устройств можно загрузить и проверить во время реализации.

В моделях служб или сетей могут быть заданы правила высокого уровня (например, «правила маршрутизации для исключения некоторых AS на пути между доменами» в примере на рисунке 2). Модели устройств будут соответствующим образом изменены для управления на основе правил. Правила можно также применять для автоматизации телеметрии (например, правила с условиями для генерации и выталкивания новых данных телеметрии).

## 4. Функциональные блоки и взаимодействия

Архитектурные соображения раздела 3 ведут к архитектуре управления жизненным циклом, показанной на рисунке 4.

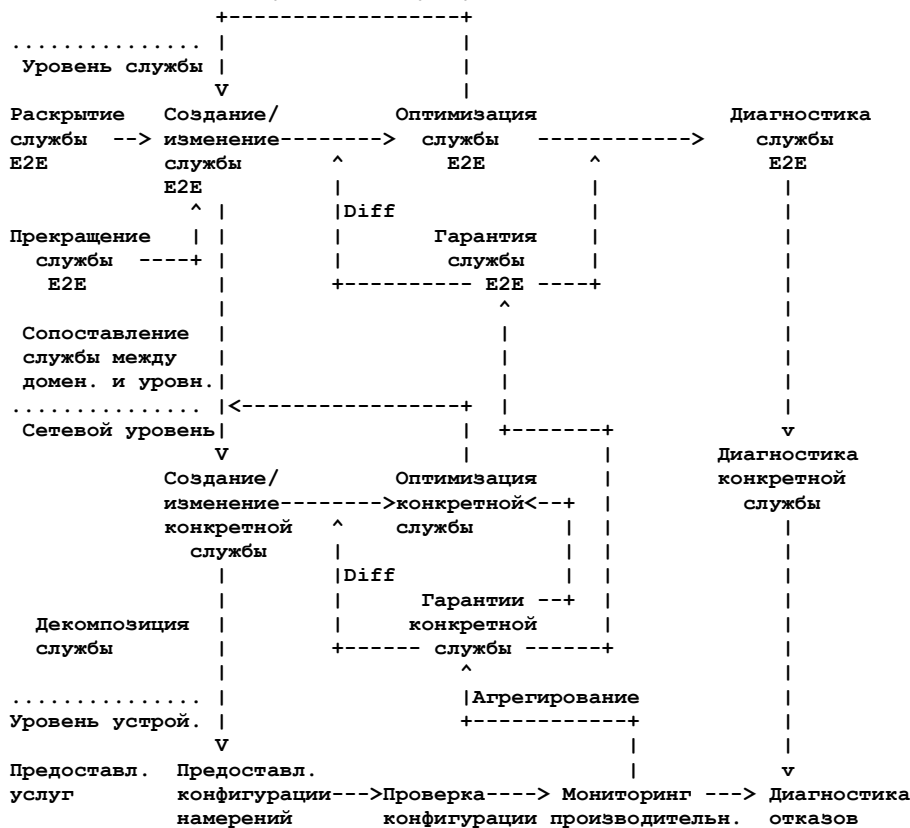


Рисунок 4. Управление жизненным циклом служб и сети.

### 4.1. Процедура управления жизненным циклом службы

Управление жизненным циклом сервиса включает сквозное управление жизненным циклом на уровне службы и связанное с технологией управление жизненным циклом сети на сетевом уровне. Сквозное управление жизненным циклом сервиса не зависит от технологии и охватывает множество сетевых доменов и/или уровней, тогда как управление жизненным циклом сервиса с учётом технологии зависит от технологического домена или от уровня.

#### 4.1.1. Раскрытие сервиса

Услугой в контексте этого документа называется та или иная форма связности между сайтами клиента и Internet или между сайтами клиента через сеть оператора и Internet. Раскрытие служб используется для нахождения услуг, предоставляемых клиентам (заказы и их обработка). Одним из примеров является возможность использования клиентом модели службы L3VPN (L3SM) для запроса услуг L3VPN путём представления абстрактных технических характеристик предполагаемой услуги между сайтами клиента.

Могут создаваться каталоги услуг для раскрытия различных служб и сведений, требуемых для вызова или заказа данной услуги.

### 4.1.2. Создание и изменение служб

Клиент обычно не знает, какие технологии доступны оператору для предоставления услуг, поэтому он не запрашивает базовую технологию и ограничивается запросами, относящимися к требуемой услуге. Этот запрос услуги можно сделать с использованием модели службы.

Получив запрос (в предположении успешной проверки подлинности и полномочий), система оркестровки (организации) должна проверить, можно ли выполнить требования, заданные в запросе услуги (достаточно ли ресурсов для выделения с запрошенными гарантиями).

Если запрос принят, система оркестровки (управления) сопоставляет этот запрос со своим представлением, которое может быть описано как связанная с технологией модель сети или набор связанных с технологией моделей устройств. Сопоставление может включать выбор сетей и технологий для использования в соответствии с запрошенными свойствами услуги.

Кроме того, для клиента может потребоваться изменение базовой сетевой инфраструктуры (например, обслуживание нового сайта клиента, добавление канала доступа или предоставление неперекрывающихся путей). Такое изменение услуги может быть внесено с той же моделью службы, которая применялась для запроса услуги.

Отказ от услуги (отзыв) рассматривается в параграфе 4.1.6. Прекращение использования услуги.

### 4.1.3. Гарантированное обслуживание

Для обеспечения гарантий на уровне службы и/или сети можно использовать телеметрию производительности (4.2.3. Мониторинг производительности). Модель телеметрии производительности можно связать с моделями служб или сетей для отслеживания производительности сети или соглашений об уровне обслуживания (Service Level Agreement или SLA).

### 4.1.4. Оптимизация службы

Оптимизация службы - это метод, с помощью которого конфигурация сети обновляется в соответствии с изменениями в сети, устранением инцидентов или новыми требованиями к услуге. Например, после создания туннеля или VPN можно собрать данные мониторинга производительности или телеметрии туннеля (VPN) и передать в систему управления. Если производительность сети не соответствует требованиям услуги, система управления может создать новые правила VPN, учитывающие требования сетевой услуги, и внедрить их в сеть.

Данные о производительности сети и правила можно промоделировать с использованием YANG. С помощью управления на основе правил можно реализовать самонастройку и само оптимизацию.

Полной оптимизацией службы можно управлять на уровне службы, а сетевой уровень отвечает за оптимизацию конкретных услуг, предоставляемых им.

### 4.1.5. Диагностика службы

OAM обеспечивает важные сетевые функции для диагностики услуг, позволяющие оператору:

- выполнять мониторинг сетевых взаимодействий (например, проверку доступности и непрерывности услуги);
- устранять неполадки (проверка и локализация отказов);
- отслеживать SLA и производительность (т. е. управлять производительностью).

Когда сеть не работает (down), диагностика службы должна сохраняться, чтобы точно указать проблему и дать рекомендации (инструкции) по восстановлению сети.

Данные диагностики службы можно смоделировать как независимые от технологии вызовы удалённых процедур (Remote Procedure Call или RPC) для протоколов OAM и независимая от технологии абстракция основных конструкций OAM для протоколов OAM [RFC8531][RFC8533]. Эти модели могут служить для обеспечения согласованной конфигурации, отчётов и предоставления механизмов OAM, применяемых для управления сетью.

Связанные с устройствами аспекты диагностики рассмотрены в параграфе 4.2.4. Диагностика отказов.

### 4.1.6. Прекращение использования услуги

Вывод службы из эксплуатации позволяет клиенту остановить службу, выведя её из активного состояния, освобождая тем самым выделенные для службы ресурсы сети. Клиенты могут также применять модель службы для отказа от подписки на услугу.

## 4.2. Процедура управления предоставлением услуги

### 4.2.1. Предоставление предусмотренной конфигурации

Предусмотренная конфигурация на уровне устройств выводится из моделей сети на уровне сети и моделей служб на уровне службы, а система пытается применить эту конфигурацию. Рассмотрим как пример модель службы L3SM для предоставления услуги L3VPN. Нужно сопоставить представление службы L3VPN, заданное моделью службы, с деталями предполагаемого представления конфигурации, заданного конкретными моделями конфигурации для элементов сети. Данные конфигурации включают:

- определение VRF, в том числе правила VPN;
- физические интерфейсы;
- уровень IP (IPv4, IPv6);
- свойства QoS, такие как классификация, профили и т. п.;
- протоколы маршрутизации - поддержка настройки всех протоколов, указанных в запросе услуги, а также правила маршрутизации, связанные с каждым из этих протоколов;
- поддержку групповой передачи;

- использование общих адресов;
- безопасность (например, контроль доступа, аутентификация, шифрование).

Эти конкретные модели конфигурации можно применить для настройки устройств провайдера (PE) и клиента (CE) внутри сайта. Например, модель политики BGP может служить для организации членства в VPN на сайтах и топологии службы VPN.

Отметим, что в сетях с унаследованными устройствами, которые поддерживают фирменные модули или не поддерживают YANG совсем, явно потребуется уровень адаптации, чтобы такие устройства можно было вовлечь в предоставление сетевых услуг.

Этот интерфейс применяется также для отзыва услуг (4.1.6. Прекращение использования услуги).

#### 4.2.2. Проверка конфигурации

Проверка предполагаемой конфигурации служит для обеспечения её установки. Например, если клиент создаёт интерфейс eth-0/0/0, но такого интерфейса физически не существует в данный момент, данные конфигурации появятся в состоянии <intended>, но не будут включены в хранилище <operational>. Дополнительные сведения о хранилищах <intended> и <operational> можно найти в параграфе 5.1 [RFC8342].

#### 4.2.3. Мониторинг производительности

Когда конфигурация применена на устройстве, хранилище <operational> содержит все рабочее состояние устройства, включая изученную (learned), системную и принятую по умолчанию конфигурацию, а также состояние системы. Однако конфигурация и состояние устройства не видны во всей сети и не могут показать, как пакеты будут пересылаться через сеть. Отсутствие понимания текущего состояния сети осложняет управление сетью.

Системе управления следует подписываться на обновления хранилищ YANG во всех сетевых устройствах для мониторинга производительности и обеспечения полной видимости сети путём агрегирования (и фильтрации) рабочих состояний из разных источников.

#### 4.2.4. Диагностика отказов

Когда конфигурация применена на устройстве, некоторые устройства могут оказаться настроенными неверно (например, не согласованы каналы на обеих сторонах сетевого соединения) или сетевые ресурсы выделены неправильно. Это может негативно сказываться на службах, не знающих сетевых первопричин.

В связанных с технологиями модулях YANG заданы зависящие от технологии узлы и RPC, которые могут использовать и расширять базовую модель, описанную в параграфе 4.1.5. Диагностика службы, для решения этих проблем. Команды RPC, получаемые зависимым от технологии узлом, можно применять для запуска связанного с технологией обмена сообщениями OAM для проверки и локализации отказов. Например, команда RPC для TRILL<sup>1</sup> MTV<sup>2</sup> [TRILL-YANG-OAM] может инициировать сообщения проверки дерева с множеством адресатов (Multi-Destination Tree Verification Message или MTVM), определённые в [RFC7455], для проверки целостности дерева распространения TRILL.

### 4.3. Многоуровневое и многодоменное представление

Многоуровневое/многодоменное сопоставление служб позволяет отобразить абстрактное сквозное представление услуги, сегментированное по уровням и/или доменам сети на специфичные для домена представления. Одним из примеров является отображение параметров службы в L3SM на параметры конфигурации, такие как различить маршрута (RD), цель маршрута (RT) и VRF с модели сети L3VPN (L3NM). Другим примером служит отображение параметров службы в L3SM на параметры туннеля TE (например, Tunnel ID) в модели TE и параметры виртуальной сети (Virtual Network или VN), такие как список точек доступа (AP) и членов VN, в модели данных YANG для операций VN [ACTN-VN-YANG].

#### 4.4. Декомпозиция службы

Декомпозиция служб позволяет разложить модели служб на уровне службы или модели сети на уровне сети на набор моделей устройств на уровне устройств. Эти модели устройств можно привязать к конкретным типам устройств или выделить в набор связанных модулей YANG по типам услуг и предлагаемым функциям и загружать во время реализации до загрузки и проверки конфигурации.

## 5. Примеры интеграции с моделью данных YANG

В последующих примерах приведены некоторые примеры интеграции с моделями данных YANG.

### 5.1. Предоставление услуг L2VPN/L3VPN

На рисунке 5 показаны этапы предоставления услуги L3VPN в рамках архитектуры автоматизации управления сетью, описанной в разделе 4. Функциональные блоки и взаимодействия.

1. Клиент запрашивает создание 2 сайтов (создание службы в параграфе 4.1.2) на основе L3SM, каждый из которых имеет одну точку подключения к сети, например,
  - Сайт А - доступ в сеть А с каналом 20 Мбит/с, класс foo, гарантированная доля полосы 10%, средняя задержка в одном направлении 70 мсек.
  - Сайт В - доступ в сеть В с каналом 30 Мбит/с, класс foo1, гарантированная доля полосы 15%, средняя задержка в одном направлении 60 мсек.
2. Оркестратор получает параметры услуги от L3SM и использует их как в ввод при сопоставлении (4.3. Многоуровневое и многодоменное представление) для трансляции в организованные параметры конфигурации (например, RD, RT и VRF), входящие в модель L3NM, заданную в [OPSAWG-L3SM-L3NM].

<sup>1</sup>Transparent Interconnection of Lots of Links - прозрачное соединение большого числа каналов.

<sup>2</sup>Multi-destination Tree Verification - проверка дерева с множеством адресатов.



- Контроллер принимает организованные параметры конфигурации в L3NM и транслирует их в организованную конфигурацию (4.4. Декомпозиция службы) элементов сети, которая является частью моделей, например, BGP, QoS, экземпляра сети, управления IP, интерфейса.

Можно использовать [UNI-TOPOLOGY] для представления, управления и контроля топологии на интерфейсе сетью-пользователь (User Network Interface или UNI).

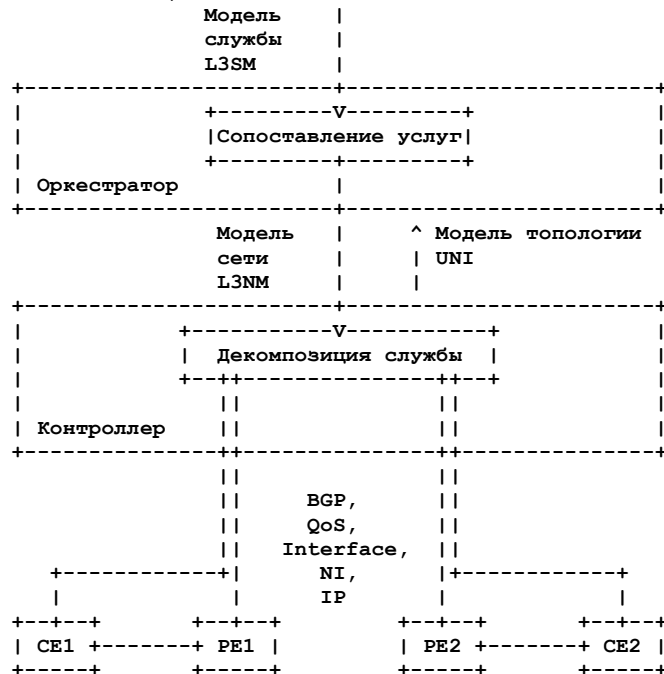


Рисунок 5. Пример предоставления услуг L3VPN (текущее).

L3NM наследует некоторые элементы данных L3SM. Тем не менее, модель L3NM, заданная в [OPSAWG-L3SM-L3NM], не раскрывает вышележащему уровню некоторые сведения, такие как возможности базовой сети (которые могут применяться для обработки заказа на услугу) и уведомления (для информирования подписчиков о конкретных событиях или нарушении SLA). Часть таких сведений может быть предоставлена с использованием, например, [OPSAWG-YANG-VPN]. Полная целевая модель показана на рисунке 6.

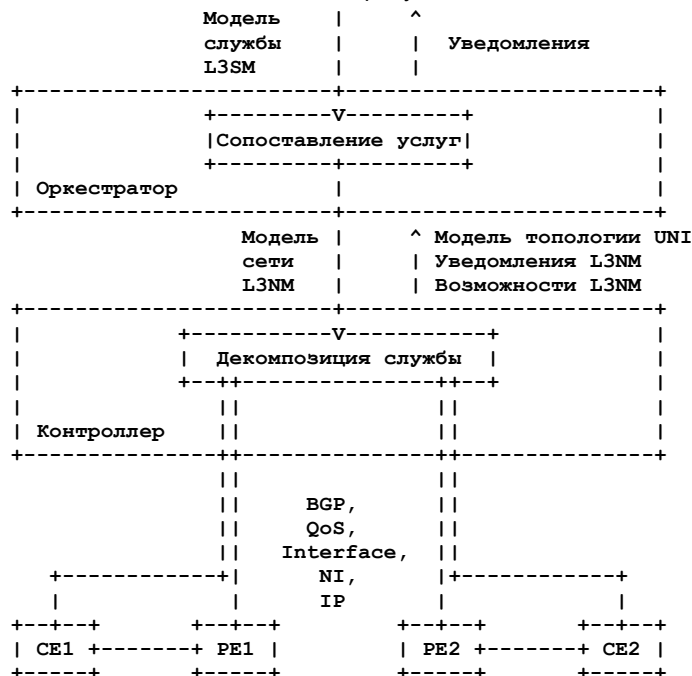


Рисунок 6. Пример предоставления услуг L3VPN (целевое).

Отметим, что похожий анализ возможен для L2VPN. Модель услуг L2VPN (L2SM) определена в [RFC8466], а модель YANG для сети L2VPN (L2NM) - в [OPSAWG-L2NM].

## 5.2. Управление жизненным циклом VN

Рисунок 7 показывает этапы предоставления услуги VN в рамках архитектуры автоматизации управления сетью, описанной в разделе 4. Функциональные блоки и взаимодействия.

- Клиент делает запрос (4.1.1. Раскрытие сервиса) на создание VN. Связи между VN, AP и членами VN определены в модели YANG VN [ACTN-VN-YANG].
- Оркестратор создаёт топологию с 1 абстрактным узлом на основе сведений из запроса.

- Клиент обменивается с оркестратором матрицей связей в топологии абстрактного узла и явными путями, используя модель топологии TE [RFC8795]. Эти сведения можно использовать для создания VN и организации туннелей между конечными точками источника и адресата (4.1.2. Создание и изменение служб).

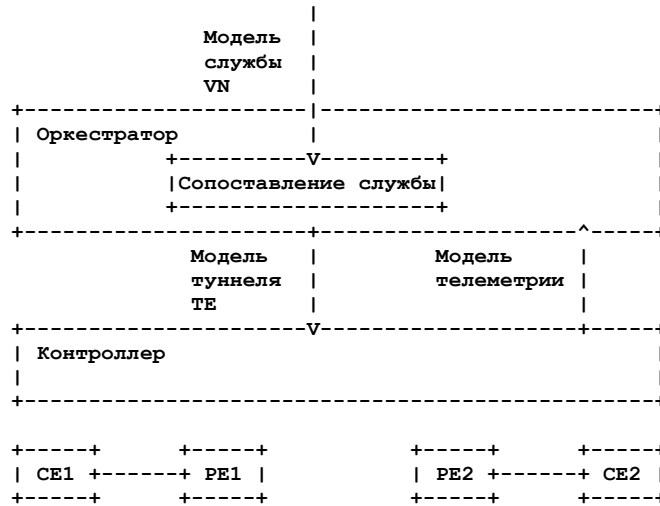


Рисунок 7. Пример предоставления услуги VN.

- Для обеспечения гарантированного обслуживания (4.1.4. Оптимизация службы) оркестратор может использовать модель телеметрии, которая дополняет модель VN и соответствующую модель туннеля TE, с целью подписки на данные измерения производительности. Контроллер может уведомлять оркестратор, передавая все изменения параметров и производительности сети, относящиеся к топологии VN и туннелям [TEAS-ACTN-PM].

### 5.3. Телеметрия по событиям в самоуправлении устройства

Рисунок 8 показывает этапы мониторинга смены состояний управляемых ресурсов сетевого устройства и обеспечивает самоуправление устройства в рамках архитектуры автоматизации управления сетью, описанной в разделе 4. Функциональные блоки и взаимодействия.

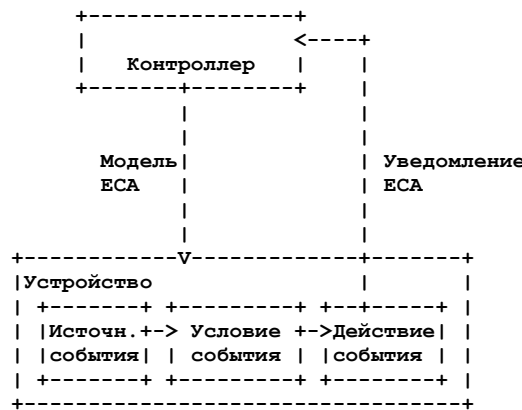


Рисунок 8. Телеметрия по событиям.

- Для контроля должного состояния устройства определён набор условий и действий, сопоставленный с событиями в сети (например, разрешать серверу NETCONF передавать обновления только при первом пересечении значением некоего порога), совместно задающие правила действий по событию (Event Condition Action или ECA) или логику управления по событиям, которая может исполняться устройством (например, [EVENT-YANG]).
- Для быстрого автоматического отклика, который может быть свойством самоуправления, контроллер выталкивает (push) правила ECA в сетевое устройство и передаёт тому логику управления сетью.
- Сетевое устройство применяет модель ECA для подписки на источник событий, например, поток событий или состояний данных хранилища, передаваемых сервером через подписку YANG-Push [RFC8641], отслеживает параметры состояния и применяет простые быстрые действия при выполнении условия, связанного с событием для параметров состояния. Уведомления ECA могут генерироваться в результате действий, основанных на подписке на поток событий или хранилище данных (4.2.3. Мониторинг производительности).

## 6. Вопросы безопасности

Многие модули YANG, упомянутые в документе, определяют схемы данных, предназначенные для доступа по протоколам управления сетью, таким как NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF служит защищённый транспорт с обязательной поддержкой SSH (Secure Shell) [RFC6242]. Нижним уровнем RESTCONF служит протокол HTTPS с обязательной поддержкой защиты на транспортном уровне (TLS) [RFC8446].

Модель управления доступом NETCONF [RFC8341] обеспечивает возможность разрешить доступ лишь определённым пользователям NETCONF или RESTCONF к заранее заданному подмножеству операций NETCONF или RESTCONF и содержимого.

Соображения безопасности упомянутых в документе технологий и протоколов рассмотрены в их спецификациях.

Для предотвращения утечки деликатных сведений и проблемы `confused deputy` [Hardy] в целом следует соблюдать особую осторожность при трансляции между уровнями (4. Функциональные блоки и взаимодействия) или агрегировании данных из разных источников. Следует проверять подлинность и полномочия, чтобы данные были доступны лишь разрешённым сущностям. Оператор сети должен применять средства защиты связанных с приватностью сведений, включая ориентированные на клиента модели.

Для обнаружения несоответствий между уровнями, которые могут быть вызваны некорректным поведением узлов, верхним уровням следует постоянно отслеживать воспринимаемые услуги (4.1.4. Оптимизация службы) и продолжать проверки для оценки соответствия предоставляемых услуг ожидаемым и соответствия данных от нижележащего уровня воспринимаемой вышележащим уровнем услуге. За такие проверки отвечает диагностика службы (4.1.5. Диагностика службы).

Если модуль YANG включает связанные с безопасностью параметры, рекомендуется включать соответствующие сведения как часть гарантии обслуживания для отслеживания корректности работы механизмов защиты.

Дополнительные соображения безопасности приведены в последующих параграфах.

## 6.1. Уровень службы

Провайдер может полагаться на услуги других провайдеров для создания составных услуг. Он должен включить соответствующие механизмы для мониторинга и обнаружения перебоев в обслуживании со стороны этих провайдеров. Характеристики перебоев обслуживания (включая среднее время между отказами и среднее время восстановления), процедуры устранения и наказания обычно включаются в договоры о предоставлении услуг (например, как описано в параграфе 2.1 [RFC4176]). Таким способом обнаруживаются партнёры с некорректным поведением и применяются соответствующие меры воздействия.

Коммуникационные протоколы, применяемые в модели службы между клиентом и оператором, не рассматриваются здесь. Соответствующие соображения безопасности должны быть рассмотрены в спецификации этих протоколов.

## 6.2. Уровень сети

Ниже указаны вопросы безопасности, связанные с сетевым уровнем.

- Контроллер может создавать петли пересылки, неверно настроив узлы базовой сети. Рекомендуется проверять статус путей пересылки регулярно или после изменений в процессе маршрутизации или пересылки. Такие проверки можно инициировать с уровня службы средствами, описанными в 4.1.5. Диагностика службы.
- Некоторые модели служб могут включать положение об изоляции трафика, которое передаётся на сетевой уровень для выполнения там (и в вовлечённых устройствах сети) связанных с технологией действий, позволяющих предотвратить доступ неуполномоченных сторон к трафику. В частности, модели сети могут указывать, включено ли шифрование, а также поддерживаемые схемы и параметры шифрования, если оно применяется. См., например, функцию шифрования, определённое в [OPSAWG-VPN-COMMON] и её применение в [OPSAWG-L3SM-L3NM].

## 6.3. Уровень устройства

Операторам следует отслеживать и проверять свои сети для обнаружения некорректного поведения узлов и других аномалий. Для этого можно использовать, например, OAM, как указано в параграфе 4.1.5. Диагностика службы.

Для доступа к некоторым данным требуется определённый уровень привилегий. Устройства должны проверять наличие требуемых прав, прежде чем предоставлять доступ к конкретным данным и выполнять конкретные действия.

## 7. Взаимодействие с IANA

Этот документ не требует действий IANA.

## 8. Литература

### 8.1. Нормативные документы

- [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>>.
- [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>>.
- [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>>.
- [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>>.

### 8.2. Дополнительная литература

- [ACTN-VN-YANG] Lee, Y., Dhody, D., Ceccarelli, D., Bryskin, I., and B. Y. Yoon, "A YANG Data Model for VN Operation", Work in Progress, Internet-Draft, draft-ietf-teas-actn-vn-yang-10, 2 November 2020, <<https://tools.ietf.org/html/draft-ietf-teas-actn-vn-yang-10>>.

[BFD-YANG]	Rahman, R., Zheng, L., Jethanandani, M., Pallagatti, S., and G. Mirsky, "YANG Data Model for Bidirectional Forwarding Detection (BFD)", Work in Progress <sup>1</sup> , Internet-Draft, draft-ietf-bfd-yang-17, 2 August 2018, < <a href="https://tools.ietf.org/html/draft-ietf-bfd-yang-17">https://tools.ietf.org/html/draft-ietf-bfd-yang-17</a> >.
[DOTS-DDOS]	Boucadair, M., Shallow, J., and T. Reddy.K, "Distributed Denial-of-Service Open Threat Signaling (DOTS) Signal Channel Specification", Work in Progress <sup>2</sup> , Internet-Draft, draft-ietf-dots-rfc8782-bis-04, 3 December 2020, < <a href="https://tools.ietf.org/html/draft-ietf-dots-rfc8782-bis-04">https://tools.ietf.org/html/draft-ietf-dots-rfc8782-bis-04</a> >.
[EVENT-YANG]	Wu, Q., Bryskin, I., Birkholz, H., Liu, X., and B. Claise, "A YANG Data model for ECA Policy Management", Work in Progress, Internet-Draft, draft-www-netmod-event-yang-10, 1 November 2020, < <a href="https://tools.ietf.org/html/draft-www-netmod-event-yang-10">https://tools.ietf.org/html/draft-www-netmod-event-yang-10</a> >.
[EVPN-YANG]	Brissette, P., Shah, H., Hussain, I., Tiruveedhula, K., and J. Rabadan, "Yang Data Model for EVPN", Work in Progress, Internet-Draft, draft-ietf-bess-evpn-yang-07, 11 March 2019, < <a href="https://tools.ietf.org/html/draft-ietf-bess-evpn-yang-07">https://tools.ietf.org/html/draft-ietf-bess-evpn-yang-07</a> >.
[Hardy]	Hardy, N., "The Confused Deputy: (or why capabilities might have been invented)", DOI 10.1145/54289.871709, October 1988, < <a href="https://dl.acm.org/doi/10.1145/54289.871709">https://dl.acm.org/doi/10.1145/54289.871709</a> >.
[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-10, 15 November 2020, < <a href="https://tools.ietf.org/html/draft-ietf-idr-bgp-model-10">https://tools.ietf.org/html/draft-ietf-idr-bgp-model-10</a> >.
[IPPM]	IANA, "Performance Metrics", March 2020, < <a href="https://www.iana.org/assignments/performance-metrics/performance-metrics.xhtml">https://www.iana.org/assignments/performance-metrics/performance-metrics.xhtml</a> >.
[L2VPN-YANG]	Shah, H., Brissette, P., Chen, I., Hussain, I., Wen, B., and K. Tiruveedhula, "YANG Data Model for MPLS-based L2VPN", Work in Progress, Internet-Draft, draft-ietf-bess-l2vpn-yang-10, 2 July 2019, < <a href="https://tools.ietf.org/html/draft-ietf-bess-l2vpn-yang-10">https://tools.ietf.org/html/draft-ietf-bess-l2vpn-yang-10</a> >.
[L3VPN-YANG]	Jain, D., Patel, K., Brissette, P., Li, Z., Zhuang, S., Liu, X., Haas, J., Esale, S., and B. Wen, "Yang Data Model for BGP/MPLS L3 VPNs", Work in Progress, Internet-Draft, draft-ietf-bess-l3vpn-yang-04, 19 October 2018, < <a href="https://tools.ietf.org/html/draft-ietf-bess-l3vpn-yang-04">https://tools.ietf.org/html/draft-ietf-bess-l3vpn-yang-04</a> >.
[METRIC-METHOD]	Morton, A., Geib, R., and L. Ciavattone, "Metrics and Methods for One-way IP Capacity", Work in Progress <sup>3</sup> , Internet-Draft, draft-ietf-ippm-capacity-metric-method-04, 10 September 2020, < <a href="https://tools.ietf.org/html/draft-ietf-ippm-capacity-metric-method-04">https://tools.ietf.org/html/draft-ietf-ippm-capacity-metric-method-04</a> >.
[MVPN-YANG]	Liu, Y., Guo, F., Litkowski, S., Liu, X., Kebler, R., and M. Sivakumar, "Yang Data Model for Multicast in MPLS/BGP IP VPNs", Work in Progress, Internet-Draft, draft-ietf-bess-mvpn-yang-04, 30 June 2020, < <a href="https://tools.ietf.org/html/draft-ietf-bess-mvpn-yang-04">https://tools.ietf.org/html/draft-ietf-bess-mvpn-yang-04</a> >.
[NETMOD-MODEL]	Clarke, J. and B. Claise, "YANG module for yangcatalog.org", Work in Progress, Internet-Draft, draft-clacla-netmod-model-catalog-03, 3 April 2018, < <a href="https://tools.ietf.org/html/draft-clacla-netmod-model-catalog-03">https://tools.ietf.org/html/draft-clacla-netmod-model-catalog-03</a> >.
[OPSAWG-L2NM]	Barguil, S., Dios, O. G. D., Boucadair, M., Munoz, L. A., Jalil, L., and J. Ma, "A Layer 2 VPN Network YANG Model", Work in Progress <sup>4</sup> , Internet-Draft, draft-ietf-opsawg-l2nm-01, 2 November 2020, < <a href="https://tools.ietf.org/html/draft-ietf-opsawg-l2nm-01">https://tools.ietf.org/html/draft-ietf-opsawg-l2nm-01</a> >.
[OPSAWG-L3SM-L3NM]	Barguil, S., Dios, O. G. D., Boucadair, M., Munoz, L. A., and A. Aguado, "A Layer 3 VPN Network YANG Model", Work in Progress <sup>5</sup> , Internet-Draft, draft-ietf-opsawg-l3sm-l3nm-05, 16 October 2020, < <a href="https://tools.ietf.org/html/draft-ietf-opsawg-l3sm-l3nm-05">https://tools.ietf.org/html/draft-ietf-opsawg-l3sm-l3nm-05</a> >.
[OPSAWG-VPN-COMMON]	Barguil, S., Dios, O. G. D., Boucadair, M., and Q. Wu, "A Layer 2/3 VPN Common YANG Model", Work in Progress <sup>6</sup> , Internet-Draft, draft-ietf-opsawg-vpn-common-03, 14 January 2021, < <a href="https://tools.ietf.org/html/draft-ietf-opsawg-vpn-common-03">https://tools.ietf.org/html/draft-ietf-opsawg-vpn-common-03</a> >.
[OPSAWG-YANG-VPN]	Wu, B., Wu, Q., Boucadair, M., Dios, O. G. D., Wen, B., Liu, C., and H. Xu, "A YANG Model for Network and VPN Service Performance Monitoring", Work in Progress, Internet-Draft, draft-www-opsawg-yang-vpn-service-pm-03, 21 January 2021, < <a href="https://tools.ietf.org/html/draft-www-opsawg-yang-vpn-service-pm-03">https://tools.ietf.org/html/draft-www-opsawg-yang-vpn-service-pm-03</a> >.
[PIM-YANG]	Liu, X., McAllister, P., Peter, A., Sivakumar, M., Liu, Y., and F. Hu, "A YANG Data Model for Protocol Independent Multicast (PIM)", Work in Progress <sup>7</sup> , Internet-Draft, draft-ietf-pim-yang-17, 19 May 2018, < <a href="https://tools.ietf.org/html/draft-ietf-pim-yang-17">https://tools.ietf.org/html/draft-ietf-pim-yang-17</a> >.
[QOS-MODEL]	Choudhary, A., Jethanandani, M., Strahle, N., Aries, E., and I. Chen, "YANG Model for QoS", Work in Progress, Internet-Draft, draft-ietf-rtgwg-qos-model-02, 9 July 2020, < <a href="https://tools.ietf.org/html/draft-ietf-rtgwg-qos-model-02">https://tools.ietf.org/html/draft-ietf-rtgwg-qos-model-02</a> >.
[RFC4176]	El Mghazli, Y., Ed., Nadeau, T., Boucadair, M., Chan, K., and A. Gonguet, "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management", RFC 4176, DOI 10.17487/RFC4176, October 2005, < <a href="https://www.rfc-editor.org/info/rfc4176">https://www.rfc-editor.org/info/rfc4176</a> >.
[RFC4364]	Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, < <a href="https://www.rfc-editor.org/info/rfc4364">https://www.rfc-editor.org/info/rfc4364</a> >.

<sup>1</sup>Опубликовано в RFC 9127. Прим. перев.

<sup>2</sup>Опубликовано в RFC 9132. Прим. перев.

<sup>3</sup>Опубликовано в RFC 9097. Прим. перев.

<sup>4</sup>Опубликовано в RFC 9291. Прим. перев.

<sup>5</sup>Опубликовано в RFC 9182. Прим. перев.

<sup>6</sup>Опубликовано в RFC 9181. Прим. перев.

<sup>7</sup>Опубликовано в RFC 9128. Прим. перев.

- [RFC4664] Andersson, L., Ed. and E. Rosen, Ed., "Framework for Layer 2 Virtual Private Networks (L2VPNs)", [RFC 4664](#), DOI 10.17487/RFC4664, September 2006, <<https://www.rfc-editor.org/info/rfc4664>>.
- [RFC4761] Kompella, K., Ed. and Y. Rekhter, Ed., "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling", [RFC 4761](#), DOI 10.17487/RFC4761, January 2007, <<https://www.rfc-editor.org/info/rfc4761>>.
- [RFC4762] Lasserre, M., Ed. and V. Kompella, Ed., "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling", [RFC 4762](#), DOI 10.17487/RFC4762, January 2007, <<https://www.rfc-editor.org/info/rfc4762>>.
- [RFC5136] Chimento, P. and J. Ishac, "Defining Network Capacity", RFC 5136, DOI 10.17487/RFC5136, February 2008, <<https://www.rfc-editor.org/info/rfc5136>>.
- [RFC5486] Malas, D., Ed. and D. Meyer, Ed., "Session Peering for Multimedia Interconnect (SPEERMINT) Terminology", RFC 5486, DOI 10.17487/RFC5486, March 2009, <<https://www.rfc-editor.org/info/rfc5486>>.
- [RFC5880] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", [RFC 5880](#), DOI 10.17487/RFC5880, June 2010, <<https://www.rfc-editor.org/info/rfc5880>>.
- [RFC6406] Malas, D., Ed. and J. Livingood, Ed., "Session PEERING for Multimedia INTERconnect (SPEERMINT) Architecture", RFC 6406, DOI 10.17487/RFC6406, November 2011, <<https://www.rfc-editor.org/info/rfc6406>>.
- [RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", [RFC 7149](#), DOI 10.17487/RFC7149, March 2014, <<https://www.rfc-editor.org/info/rfc7149>>.
- [RFC7224] Bjorklund, M., "IANA Interface Type YANG Module", [RFC 7224](#), DOI 10.17487/RFC7224, May 2014, <<https://www.rfc-editor.org/info/rfc7224>>.
- [RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", [RFC 7276](#), DOI 10.17487/RFC7276, June 2014, <<https://www.rfc-editor.org/info/rfc7276>>.
- [RFC7297] Boucadair, M., Jacquenet, C., and N. Wang, "IP Connectivity Provisioning Profile (CPP)", RFC 7297, DOI 10.17487/RFC7297, July 2014, <<https://www.rfc-editor.org/info/rfc7297>>.
- [RFC7317] Bierman, A. and M. Bjorklund, "A YANG Data Model for System Management", [RFC 7317](#), DOI 10.17487/RFC7317, August 2014, <<https://www.rfc-editor.org/info/rfc7317>>.
- [RFC7455] Senevirathne, T., Finn, N., Salam, S., Kumar, D., Eastlake 3rd, D., Aldrin, S., and Y. Li, "Transparent Interconnection of Lots of Links (TRILL): Fault Management", RFC 7455, DOI 10.17487/RFC7455, March 2015, <<https://www.rfc-editor.org/info/rfc7455>>.
- [RFC7665] Halpern, J., Ed. and C. Pignataro, Ed., "Service Function Chaining (SFC) Architecture", RFC 7665, DOI 10.17487/RFC7665, October 2015, <<https://www.rfc-editor.org/info/rfc7665>>.
- [RFC7679] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Delay Metric for IP Performance Metrics (IPPM)", STD 81, [RFC 7679](#), DOI 10.17487/RFC7679, January 2016, <<https://www.rfc-editor.org/info/rfc7679>>.
- [RFC7680] Almes, G., Kalidindi, S., Zekauskas, M., and A. Morton, Ed., "A One-Way Loss Metric for IP Performance Metrics (IPPM)", STD 82, [RFC 7680](#), DOI 10.17487/RFC7680, January 2016, <<https://www.rfc-editor.org/info/rfc7680>>.
- [RFC8077] Martini, L., Ed. and G. Heron, Ed., "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", STD 84, [RFC 8077](#), DOI 10.17487/RFC8077, February 2017, <<https://www.rfc-editor.org/info/rfc8077>>.
- [RFC8194] Schoenwaelder, J. and V. Bajpai, "A YANG Data Model for LMAP Measurement Agents", RFC 8194, DOI 10.17487/RFC8194, August 2017, <<https://www.rfc-editor.org/info/rfc8194>>.
- [RFC8199] Bogdanovic, D., Claise, B., and C. Moberg, "YANG Module Classification", [RFC 8199](#), DOI 10.17487/RFC8199, July 2017, <<https://www.rfc-editor.org/info/rfc8199>>.
- [RFC8299] Wu, Q., Ed., Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8299, DOI 10.17487/RFC8299, January 2018, <<https://www.rfc-editor.org/info/rfc8299>>.
- [RFC8309] Wu, Q., Liu, W., and A. Farrel, "Service Models Explained", [RFC 8309](#), DOI 10.17487/RFC8309, January 2018, <<https://www.rfc-editor.org/info/rfc8309>>.
- [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>>.
- [RFC8345] Clemm, A., Medved, J., Varga, R., Bahadur, N., Ananthakrishnan, H., and X. Liu, "A YANG Data Model for Network Topologies", [RFC 8345](#), DOI 10.17487/RFC8345, March 2018, <<https://www.rfc-editor.org/info/rfc8345>>.

- [RFC8346] Clemm, A., Medved, J., Varga, R., Liu, X., Ananthkrishnan, H., and N. Bahadur, "A YANG Data Model for Layer 3 Topologies", [RFC 8346](#), DOI 10.17487/RFC8346, March 2018, <<https://www.rfc-editor.org/info/rfc8346>>.
- [RFC8348] Bierman, A., Bjorklund, M., Dong, J., and D. Romascanu, "A YANG Data Model for Hardware Management", [RFC 8348](#), DOI 10.17487/RFC8348, March 2018, <<https://www.rfc-editor.org/info/rfc8348>>.
- [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>>.
- [RFC8466] Wen, B., Fioccola, G., Ed., Xie, C., and L. Jalil, "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery", [RFC 8466](#), DOI 10.17487/RFC8466, October 2018, <<https://www.rfc-editor.org/info/rfc8466>>.
- [RFC8512] Boucadair, M., Ed., Sivakumar, S., Jacquenet, C., Vinapamula, S., and Q. Wu, "A YANG Module for Network Address Translation (NAT) and Network Prefix Translation (NPT)", RFC 8512, DOI 10.17487/RFC8512, January 2019, <<https://www.rfc-editor.org/info/rfc8512>>.
- [RFC8513] Boucadair, M., Jacquenet, C., and S. Sivakumar, "A YANG Data Model for Dual-Stack Lite (DS-Lite)", RFC 8513, DOI 10.17487/RFC8513, January 2019, <<https://www.rfc-editor.org/info/rfc8513>>.
- [RFC8519] Jethanandani, M., Agarwal, S., Huang, L., and D. Blair, "YANG Data Model for Network Access Control Lists (ACLs)", [RFC 8519](#), DOI 10.17487/RFC8519, March 2019, <<https://www.rfc-editor.org/info/rfc8519>>.
- [RFC8525] Bierman, A., Bjorklund, M., Schoenwaelder, J., Watsen, K., and R. Wilton, "YANG Library", [RFC 8525](#), DOI 10.17487/RFC8525, March 2019, <<https://www.rfc-editor.org/info/rfc8525>>.
- [RFC8528] Bjorklund, M. and L. Lhotka, "YANG Schema Mount", [RFC 8528](#), DOI 10.17487/RFC8528, March 2019, <<https://www.rfc-editor.org/info/rfc8528>>.
- [RFC8529] Berger, L., Hopps, C., Lindem, A., Bogdanovic, D., and X. Liu, "YANG Data Model for Network Instances", [RFC 8529](#), DOI 10.17487/RFC8529, March 2019, <<https://www.rfc-editor.org/info/rfc8529>>.
- [RFC8530] Berger, L., Hopps, C., Lindem, A., Bogdanovic, D., and X. Liu, "YANG Model for Logical Network Elements", [RFC 8530](#), DOI 10.17487/RFC8530, March 2019, <<https://www.rfc-editor.org/info/rfc8530>>.
- [RFC8531] Kumar, D., Wu, Q., and Z. Wang, "Generic YANG Data Model for Connection-Oriented Operations, Administration, and Maintenance (OAM) Protocols", [RFC 8531](#), DOI 10.17487/RFC8531, April 2019, <<https://www.rfc-editor.org/info/rfc8531>>.
- [RFC8532] Kumar, D., Wang, Z., Wu, Q., Ed., Rahman, R., and S. Raghavan, "Generic YANG Data Model for the Management of Operations, Administration, and Maintenance (OAM) Protocols That Use Connectionless Communications", [RFC 8532](#), DOI 10.17487/RFC8532, April 2019, <<https://www.rfc-editor.org/info/rfc8532>>.
- [RFC8533] Kumar, D., Wang, M., Wu, Q., Ed., Rahman, R., and S. Raghavan, "A YANG Data Model for Retrieval Methods for the Management of Operations, Administration, and Maintenance (OAM) Protocols That Use Connectionless Communications", [RFC 8533](#), DOI 10.17487/RFC8533, April 2019, <<https://www.rfc-editor.org/info/rfc8533>>.
- [RFC8632] Vallin, S. and M. Bjorklund, "A YANG Data Model for Alarm Management", [RFC 8632](#), DOI 10.17487/RFC8632, September 2019, <<https://www.rfc-editor.org/info/rfc8632>>.
- [RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", [RFC 8641](#), DOI 10.17487/RFC8641, September 2019, <<https://www.rfc-editor.org/info/rfc8641>>.
- [RFC8652] Liu, X., Guo, F., Sivakumar, M., McAllister, P., and A. Peter, "A YANG Data Model for the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD)", RFC 8652, DOI 10.17487/RFC8652, November 2019, <<https://www.rfc-editor.org/info/rfc8652>>.
- [RFC8675] Boucadair, M., Farrer, I., and R. Asati, "A YANG Data Model for Tunnel Interface Types", [RFC 8675](#), DOI 10.17487/RFC8675, November 2019, <<https://www.rfc-editor.org/info/rfc8675>>.
- [RFC8676] Farrer, I., Ed. and M. Boucadair, Ed., "YANG Modules for IPv4-in-IPv6 Address plus Port (A+P) Softwires", RFC 8676, DOI 10.17487/RFC8676, November 2019, <<https://www.rfc-editor.org/info/rfc8676>>.
- [RFC8783] Boucadair, M., Ed. and T. Reddy, K., Ed., "Distributed Denial-of-Service Open Threat Signaling (DOTS) Data Channel Specification", RFC 8783, DOI 10.17487/RFC8783, May 2020, <<https://www.rfc-editor.org/info/rfc8783>>.
- [RFC8791] Bierman, A., Björklund, M., and K. Watsen, "YANG Data Structure Extensions", [RFC 8791](#), DOI 10.17487/RFC8791, June 2020, <<https://www.rfc-editor.org/info/rfc8791>>.
- [RFC8795] Liu, X., Bryskin, I., Beeram, V., Saad, T., Shah, H., and O. Gonzalez de Dios, "YANG Data Model for Traffic Engineering (TE) Topologies", [RFC 8795](#), DOI 10.17487/RFC8795, August 2020, <<https://www.rfc-editor.org/info/rfc8795>>.
- [RFC8819] Hopps, C., Berger, L., and D. Bogdanovic, "YANG Module Tags", [RFC 8819](#), DOI 10.17487/RFC8819, January 2021, <<https://www.rfc-editor.org/info/rfc8819>>.

[RFC8944]	Dong, J., Wei, X., Wu, Q., Boucadair, M., and A. Liu, "A YANG Data Model for Layer 2 Network Topologies", <a href="#">RFC 8944</a> , DOI 10.17487/RFC8944, November 2020, < <a href="https://www.rfc-editor.org/info/rfc8944">https://www.rfc-editor.org/info/rfc8944</a> >.
[RFC8960]	Saad, T., Raza, K., Gandhi, R., Liu, X., and V. Beeram, "A YANG Data Model for MPLS Base", RFC 8960, DOI 10.17487/RFC8960, December 2020, < <a href="https://www.rfc-editor.org/info/rfc8960">https://www.rfc-editor.org/info/rfc8960</a> >.
[RTGWG-POLICY]	Qu, Y., Tantsura, J., Lindem, A., and X. Liu, "A YANG Data Model for Routing Policy", Work in Progress <sup>1</sup> , Internet-Draft, draft-ietf-rtwgw-policy-model-27, 10 January 2021, < <a href="https://tools.ietf.org/html/draft-ietf-rtwgw-policy-model-27">https://tools.ietf.org/html/draft-ietf-rtwgw-policy-model-27</a> >.
[SNOOPING-YANG]	Zhao, H., Liu, X., Liu, Y., Sivakumar, M., and A. Peter, "A Yang Data Model for IGMP and MLD Snooping", Work in Progress <sup>2</sup> , Internet-Draft, draft-ietf-pim-igmp-ml-d-snooping-yang-18, 14 August 2020, < <a href="https://tools.ietf.org/html/draft-ietf-pim-igmp-ml-d-snooping-yang-18">https://tools.ietf.org/html/draft-ietf-pim-igmp-ml-d-snooping-yang-18</a> >.
[SPRING-SR-YANG]	Litkowski, S., Qu, Y., Lindem, A., Sarkar, P., and J. Tantsura, "YANG Data Model for Segment Routing", Work in Progress <sup>3</sup> , Internet-Draft, draft-ietf-spring-sr-yang-29, 8 December 2020, < <a href="https://tools.ietf.org/html/draft-ietf-spring-sr-yang-29">https://tools.ietf.org/html/draft-ietf-spring-sr-yang-29</a> >.
[STAMP-YANG]	Mirsky, G., Min, X., and W. S. Luo, "Simple Two-way Active Measurement Protocol (STAMP) Data Model", Work in Progress, Internet-Draft, draft-ietf-ippm-stamp-yang-06, 7 October 2020, < <a href="https://tools.ietf.org/html/draft-ietf-ippm-stamp-yang-06">https://tools.ietf.org/html/draft-ietf-ippm-stamp-yang-06</a> >.
[TEAS-ACTN-PM]	Lee, Y., Dhody, D., Karunanithi, S., Vilalta, R., King, D., and D. Ceccarelli, "YANG models for VN/TE Performance Monitoring Telemetry and Scaling Intent Autonomics", Work in Progress, Internet-Draft, draft-ietf-teas-actn-pm-telemetry-autonomics-04, 2 November 2020, < <a href="https://tools.ietf.org/html/draft-ietf-teas-actn-pm-telemetry-autonomics-04">https://tools.ietf.org/html/draft-ietf-teas-actn-pm-telemetry-autonomics-04</a> >.
[TEAS-YANG-PATH-COMP]	Busi, I., Belotti, S., Lopez, V., Sharma, A., and Y. Shi, "Yang model for requesting Path Computation", Work in Progress, Internet-Draft, draft-ietf-teas-yang-path-computation-11, 16 November 2020, < <a href="https://tools.ietf.org/html/draft-ietf-teas-yang-path-computation-11">https://tools.ietf.org/html/draft-ietf-teas-yang-path-computation-11</a> >.
[TEAS-YANG-RSVP]	Beeram, V. P., Saad, T., Gandhi, R., Liu, X., Bryskin, I., and H. Shah, "A YANG Data Model for RSVP-TE Protocol", Work in Progress, Internet-Draft, draft-ietf-teas-yang-rsvp-te-08, 9 March 2020, < <a href="https://tools.ietf.org/html/draft-ietf-teas-yang-rsvp-te-08">https://tools.ietf.org/html/draft-ietf-teas-yang-rsvp-te-08</a> >.
[TEAS-YANG-TE]	Saad, T., Gandhi, R., Liu, X., Beeram, V. P., and I. Bryskin, "A YANG Data Model for Traffic Engineering Tunnels, Label Switched Paths and Interfaces", Work in Progress, Internet-Draft, draft-ietf-teas-yang-te-25, 27 July 2020, < <a href="https://tools.ietf.org/html/draft-ietf-teas-yang-te-25">https://tools.ietf.org/html/draft-ietf-teas-yang-te-25</a> >.
[TRILL-YANG-OAM]	Kumar, D., Senevirathne, T., Finn, N., Salam, S., Xia, L., and W. Hao, "YANG Data Model for TRILL Operations, Administration, and Maintenance (OAM)", Work in Progress, Internet-Draft, draft-ietf-trill-yang-oam-05, 31 March 2017, < <a href="https://tools.ietf.org/html/draft-ietf-trill-yang-oam-05">https://tools.ietf.org/html/draft-ietf-trill-yang-oam-05</a> >.
[TWAMP-DATA-MODEL]	Civil, R., Morton, A., Rahman, R., Jethanandani, M., and K. Pentikousis, "Two-Way Active Measurement Protocol (TWAMP) Data Model", Work in Progress <sup>4</sup> , Internet-Draft, draft-ietf-ippm-twamp-yang-13, 2 July 2018, < <a href="https://tools.ietf.org/html/draft-ietf-ippm-twamp-yang-13">https://tools.ietf.org/html/draft-ietf-ippm-twamp-yang-13</a> >.
[UNI-TOPOLOGY]	Dios, O. G. D., Barguil, S., Wu, Q., and M. Boucadair, "A YANG Model for User-Network Interface (UNI) Topologies", Work in Progress, Internet-Draft, draft-ogondio-opsawg-uni-topology-01, 2 April 2020, < <a href="https://tools.ietf.org/html/draft-ogondio-opsawg-uni-topology-01">https://tools.ietf.org/html/draft-ogondio-opsawg-uni-topology-01</a> >.

## Приложение А. Обзор примеров многоуровневых модулей YANG

В этом приложении рассмотрены модели данных YANG, которые могут служить для предоставления услуг связности. Эти модели можно классифицировать как модели служб, сетей или устройств.

Приложение не включает список инструментов и механизмов, применяемых в конкретных доменах управления сетями и службами, такие списки можно найти в [RFC7276] и других документах.

Читатель может обратиться к каталогу YANG (<<https://www.yangcatalog.org>>) или общедоступному репозиторию Github YANG (<<https://github.com/YangModels/yang>>) для поиска интересующих модулей YANG. Каталог YANG включает некоторые метаданные, указывающие тип модуля (module-classification) [NETMOD-MODEL]. Отметим, что механизм, заданный в [RFC8819] позволяет связывать с модулями YANG теги, позволяющие классифицировать модули.

### А.1. Модели служб - определения и примеры

Как описано в [RFC8309], службой считается «та или иная форма связности сайтов клиента с Internet или соединения сайтов клиента через сеть оператора и Internet». Более конкретно, услугу связности IP можно определить как способность передачи трафика IP, характеризуемого квартетом (Source Nets, Destination Nets, Guarantees, Scope), где Source Nets указывает группу индивидуальных адресов, Destination Nets - группу индивидуальных и/или групповых адресов IP, Guarantees отражает гарантии (например, в терминах QoS, производительности и доступности) надлежащей пересылки трафика получателю Destination [RFC7297]. Scope указывает сетевой периметр (например, между маршрутизаторами PE и узлами клиента), где гарантии должны быть предоставлены. Например,

- L3SM [RFC8299] определяет услугу L3VPN, заказываемую клиентом у оператора сети;
- L2SM [RFC8466] определяет услугу L2VPN, заказываемую клиентом у оператора сети;
- модель VN [ACTN-VN-YANG] предоставляет модель данных YANG, применимую к любому режиму работы VN.

<sup>1</sup>Опубликовано в [RFC 9067](#). Прим. перев.

<sup>2</sup>Опубликовано в [RFC 9166](#). Прим. перев.

<sup>3</sup>Опубликовано в [RFC 9020](#). Прим. перев.

<sup>4</sup>Опубликовано в [RFC 8913](#). Прим. перев.

## А.2. Монтирование схемы

Модульность и расширяемость были основными принципами разработки языка моделирования данных YANG. В результате один и тот же модуль YANG можно сочетать с разными наборами иных модулей для формирования модели данных, приспособленной к требованиям конкретного варианта применения. В [RFC8528] задан механизм, названный монтированием схемы (schema mount), который позволяет смонтировать модель данных, состоящую из любого числа модулей YANG в конкретном месте другой (родительской) схемы.

## А.3. Модели служб - примеры

L2NM [OPSAWG-L2NM] и L3NM [OPSAWG-L3SM-L3NM] являются примерами моделей YANG для сети. На рисунке 9 показан набор дополнительных моделей сетей, таких как модели топологии и туннелей.

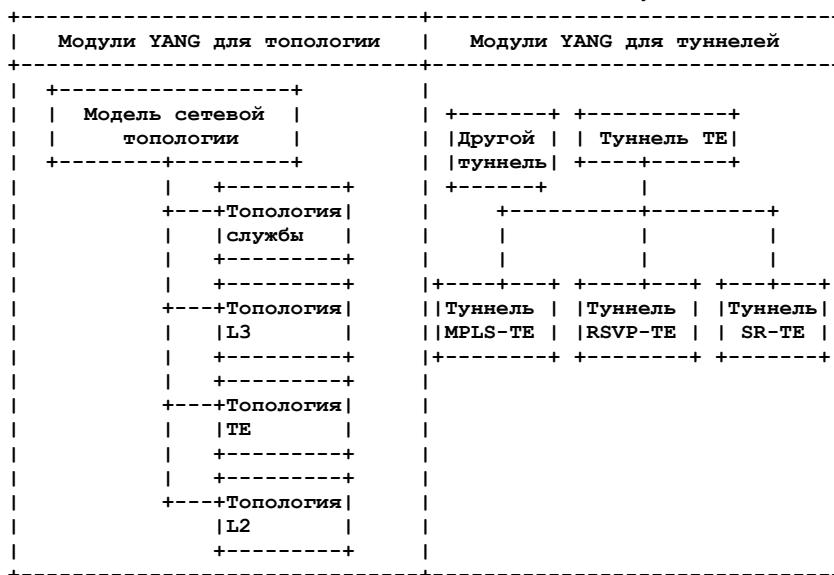


Рисунок 9. Примеры ориентированных на ресурсы моделей сетей.

Ниже приведены примеры топологических модулей YANG.

### Модель топологии сети

В [RFC8345] определена модель для топологии сети и инвентаризации. Данные топологии включают ресурсы каналов, узлов и точек завершения.

### Модель топологии TE

В [RFC8795] определена модель данных YANG для представления топологии TE и манипуляций с ней. Этот модуль является расширением модуля топологии из [RFC8345] и включает содержимое, связанное с топологией TE. Модель содержит не связанные с технологией блоки построения топологии TE, которые можно дополнять и применять в других моделях топологии TE, связанных с технологией.

### Модель топологии L3

В [RFC8346] определена модель данных YANG для манипуляций с топологией L3, являющаяся расширением модели из [RFC8345] и включающая детали, связанные в топологией L3.

### Модель топологии L2

В [RFC8944] определена модель данных YANG для манипуляций с топологией L2, являющаяся расширением модели из [RFC8345] и включающая детали, связанные в топологией L2.

Ниже приведены примеры модулей YANG для туннелей.

### Идентификаторы туннелей

В [RFC8675] задан набор идентификаторов YANG для туннелей, служащих типами интерфейсов для туннелей.

### Модель туннелей TE

В [TEAS-YANG-TE] задан модуль YANG для настройки и управления интерфейсами и туннелями TE, а также LSP.

### Модель туннелей SR TE

[TEAS-YANG-TE] дополняет базовые модели TE и MPLS-TE, задавая модуль данных YANG, связанный с SR-TE.

### Модель MPLS-TE

[TEAS-YANG-TE] дополняет базовые модели TE и MPLS-TE, задавая модуль данных YANG для конфигурации и состояния MPLS-TE, RPC и уведомлений.

### Модель MPLS RSVP-TE

[TEAS-YANG-RSVP] дополняет базовый модуль RSVP-TE параметрами для настройки и управления сигнализацией MPLS RSVP-TE LSP.

Ниже перечислены другие примеры моделей для сетей.

### Модель API расчёта путей

В [TEAS-YANG-PATH-COMP] задан модуль YANG для RPC без учёта состояния, дополняющий решение с учётом состояний из [TEAS-YANG-TE].

### Модели OAM (включая контроль отказов и мониторинг производительности)

В [RFC8532] задан базовый модуль YANG для управления протоколами OAM, не использующими явных соединений. В [RFC8533] задан модуль YANG для извлечения из протоколов OAM без организации соединений. [RFC8531] определяет базовый модуль YANG для ориентированных на соединения протоколов OAM. Имеется 3 модели, предназначенных для предоставления согласованных отчётов, конфигурации и представлений OAM с организацией соединений и без них.



Мониторинг сигналов тревоги является важной частью сетевого мониторинга. Необработанные (Raw) сигналы тревоги от сетевых устройств не всегда указывают статус сетевых услуг или место основной причины отказа. В [RFC8632] задан модуль YANG для сигналов тревоги.

## А.4. Модели устройств - примеры

Модели элементов сети (Рисунок 10) служат для описания возможной реализации службы путём активации и настройки набора функций (включённых на одном или нескольких устройствах, или размещённых в облачной инфраструктуре), вовлечённых в предоставление услуги. Например, служба L3VPN включает множество PE и требует манипуляция с указанными ниже модулями.

- Управление маршрутизацией [RFC8349].
- BGP [IDR-BGP-MODEL].
- PIM [PIM-YANG].
- Управление NAT [RFC8512].
- Управление QoS [QOS-MODEL].
- ACL [RFC8519].

На рисунке 10 в качестве примера указаны заданные IETF модели данных.

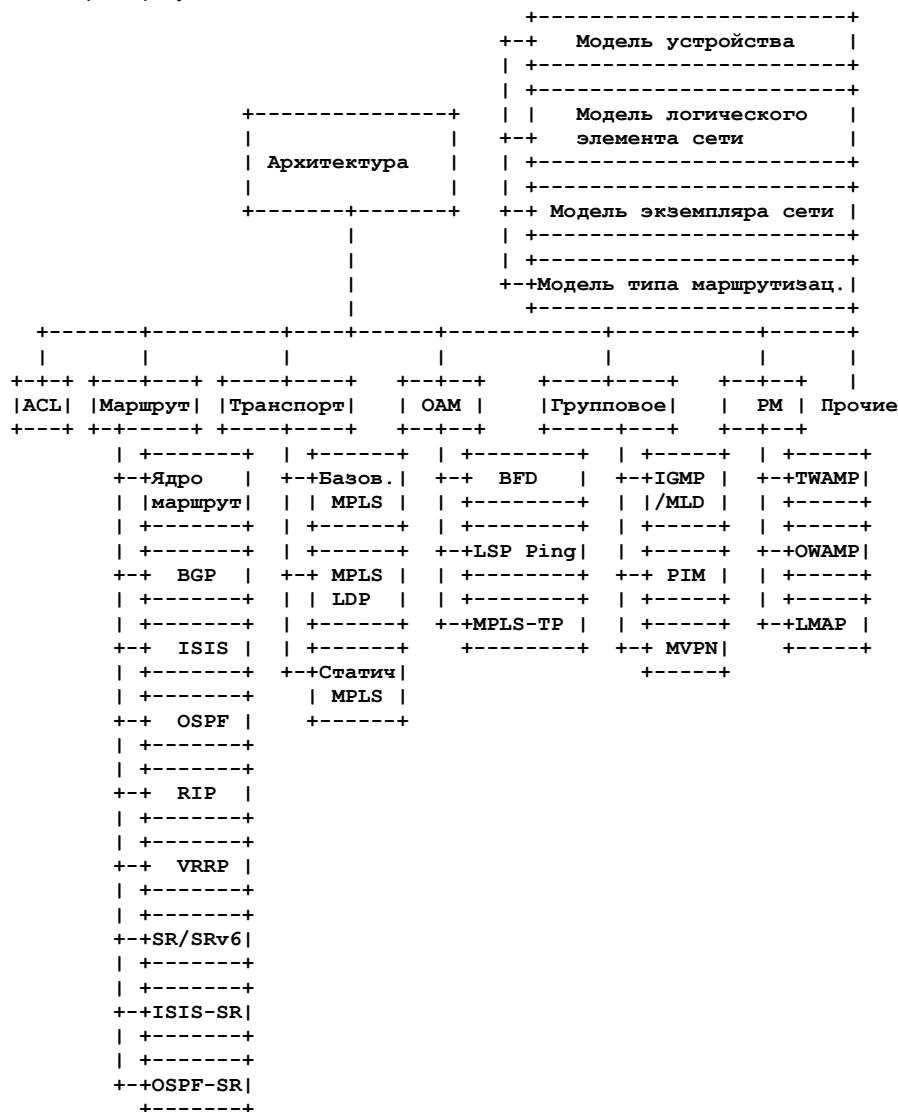


Рисунок 10. Обзор моделей элементов сети.

### А.4.1. Модели для компоновки

#### Модель логического элемента сети

В [RFC8530] задана модель логического элемента сети, которую можно применять для управления разделением логических ресурсов, которые могут присутствовать в сетевом устройстве. Примерами разделения логических ресурсов служат логические системы и логические маршрутизаторы.

#### Модель экземпляра сети

В [RFC8529] задан модуль для экземпляра сети, который может служить для управления распределением виртуальных ресурсов, которые могут присутствовать в сетевом устройстве. Примерами разделения таких ресурсов являются экземпляры VRF и виртуальных коммутаторов (Virtual Switch Instance или VSI).

### А.4.2. Управление устройствами

Ниже указаны некоторые модули YANG, которые могут служить для управления устройствами.

- В [RFC8348] определён модуль YANG для управления оборудованием.

- В [RFC7317] задан модуль YANG ieff-system со множеством функций, таких как настройка и мониторинг системы или идентификация операций управления системой (например, отключение - shutdown, перезапуск, установка времени).
- В [RFC8341] задан модуль YANG для контроля доступа к конфигурации сети.

### **A.4.3. Управление интерфейсом**

Ниже приведён список модулей YANG, которые могут служить для управления интерфейсами.

- [RFC7224] задаёт модуль YANG с определениями типов интерфейсов.
- [RFC8343] задаёт модуль YANG для управления сетевыми интерфейсами.

### **A.4.4. Примеры моделей для устройств**

Ниже представлен обзор некоторых моделей для устройств, которые могут применяться в сети.

#### **L2VPN**

[L2VPN-YANG] задаёт модуль YANG для услуг L2VPN [RFC4664] и включает коммутацию между локально подключёнными устройствами. Модель L2VPN охватывает службу виртуальных частных проводов «точка-точка» (Virtual Private Wire Service или VPWS) и многоточечных виртуальных частных ЛВС (Multipoint Virtual Private LAN Service или VPLS). В этих службах применяется сигнализация для псевдопроводов через MPLS с использованием LDP [RFC8077][RFC4762] или BGP [RFC4761].

#### **EVPN**

[EVPN-YANG] определяет модуль YANG для служб Ethernet VPN. Модель не зависит от базовой сети (underlay). Она подходит для инкапсуляции MPLS и VxLAN<sup>1</sup>. Модуль не зависит от служб, включая E-LAN, E-LINE, E-TREE.

#### **L3VPN**

[L3VPN-YANG] задаёт модуль YANG, который можно применять для настройки и управления BGP L3VPN [RFC4364]. Модуль содержит связанные с VRF параметры, а также связанные с BGP параметры, применимые в L3VPN.

#### **Ядро маршрутизации**

[RFC8349] определяет модель данных YANG для ядра маршрутизации, предназначенный у качестве основы для будущих моделей, охватывающих более сложные системы маршрутизации. Предполагается, что модули YANG для других типов маршрутизации (например, VRRP, RIP, ISIS, OSPF) будут дополнять этот базовый модуль.

#### **MPLS**

[RFC8960] задаёт базовую модель для MPLS которая служит основой для настройки и управления подсистемой коммутации MPLS. Предполагается, что другие модули YANG MPLS (например, для статических MPLS LSP, LDP, RSVP-TE) будут дополнять этот базовый модуль YANG.

#### **BGP**

В [IDR-BGP-MODEL] задан модуль YANG для настройки и управления BGP, включая протокол, правила и аспекты работы в соответствии с требованиями ЦОД, операторов и контент-провайдеров.

#### **Политика маршрутизации**

[RTGWG-POLICY] определяет модуль YANG для настройки и управления политиками маршрутизации на основе опыта эксплуатации. Модуль обеспечивает базовую схему политики и может дополняться связанными с протоколами конфигурациями правил.

#### **SR/SRv6**

[SPRING-SR-YANG] задаёт модуль YANG для настройки и использования маршрутизации по сегментам.

#### **BFD**

Протокол двухстороннего обнаружения пересылки (Bidirectional Forwarding Detection или BFD) [RFC5880] применяется для определения живучести произвольных путей между системами [BFD-YANG] задаёт модуль YANG, который можно применять для настройки и управления BFD.

#### **Групповая передача**

[PIM-YANG] задаёт модуль YANG, который можно использовать для настройки и управления устройствами PIM<sup>2</sup>. В [RFC8652] определён модуль YANG, который может служить для настройки и управления устройствами IGMP<sup>3</sup> и MLD<sup>4</sup>. В [SNOOPING-YANG] задан модуль YANG, который можно применять для настройки и управления устройствами IGMP и MLD (snooping). В [MVPN-YANG] определена модель данных YANG для настройки и управления групповой передачей в MPLS/BGP IP VPN (MVPN).

#### **PM**

[TWAMP-DATA-MODEL] задаёт модель данных YANG для реализации клиента и сервера протокола двухсторонних активных измерений (Two-Way Active Measurement Protocol или TWAMP). В [STAMP-YANG] определена модель данных для реализаций Session-Sender и Session-Reflector в простом протоколе двухсторонних активных измерений (Simple Two-way Active Measurement Protocol или (STAMP), использующая YANG. В [RFC8194] задана модель данных YANG для платформ крупномасштабных измерений (Large-Scale Measurement Platform или LMAP).

#### **ACL**

ACL являются одними из базовых элементов для настройки поведения пересылки в устройствах. Они применяются во многих сетевых технологиях, таких как маршрутизация на основе правил (Policy-Based Routing), межсетевые экраны и т. п. В [RFC8519] описана модель данных YANG для базовых блоков ACL.

#### **QoS**

[QOS-MODEL] описывает модуль YANG для настройки и эксплуатации дифференцированных услуг (Differentiated Services или DS).

#### **NAT**

Для автоматизации сети и необходимости программировать функции NAT, в частности, важна модель данных YANG для настройки и управления NAT. В [RFC8512] задан модуль YANG для функции NAT, охватывающий различные варианты трансляции, такие как преобразование IPv4 в IPv4 (NAT44), трансляция адресов и протоколов от клиентов IPv6 к серверам IPv4 (Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers или

<sup>1</sup>Virtual eXtensible Local Area Network - расширяемая виртуальная частная ЛВС.

<sup>2</sup>Protocol Independent Multicast - независимая от устройств групповая передача.

<sup>3</sup>Internet Group Management Protocol - протокол управления группами Internet.

<sup>4</sup>Multicast Listener Discovery - обнаружение групповых получателей (слушателей).

NAT64), трансляторы на стороне клиента (customer-side translator или CLAT), трансляция IP/ICMP без учёта состояния (Stateless IP/ICMP Translation или SIIT), явное сопоставления адресов (Explicit Address Mapping или EAM) для SIIT, трансляция сетевых префиксов IPv6 в IPv6 (IPv6-to-IPv6 Network Prefix Translation или NPTv6), трансляция адресов плучателей (Destination NAT). В [RFC8513] задан модуль YANG для двойного стека (Dual-Stack Lite или DS-Lite).

#### **Совместное использование адресов без учёта состояния**

в [RFC8676] задан модуль YANG для совместного использования адресов и портов (Address plus Port или A+P), включая Lightweight 4over6, сопоставление адреса и порта с инкапсуляцией (Mapping of Address and Port with Encapsulation или MAP-E), сопоставление адреса и порта с применением трансляции (Mapping of Address and Port using Translation или MAP-T).

## **Благодарности**

Спасибо Joe Clark, Greg Mirsky, Shunsuke Homma, Brian Carpenter, Adrian Farrel, Christian Huitema, Tommy Pauly, Ines Robles, Olivier Augizeau за рецензии.

Большое спасибо Robert Wilton за подробную рецензию AD.

Спасибо Éric Vyncke, Roman Danyliw, Erik Kline, Benjamin Kaduk за рецензию IESG.

## **Участники работы**

### **Christian Jacquenet**

Orange  
Rennes, 35000  
France  
Email: [Christian.jacquenet@orange.com](mailto:Christian.jacquenet@orange.com)

### **Luis Miguel Contreras Murillo**

Telefonica  
Email: [luismiguel.contrerasmurillo@telefonica.com](mailto:luismiguel.contrerasmurillo@telefonica.com)

### **Oscar Gonzalez de Dios**

Telefonica

Madrid

Spain

Email: [oscar.gonzalezdedios@telefonica.com](mailto:oscar.gonzalezdedios@telefonica.com)

### **Weiqliang Cheng**

China Mobile

Email: [chengweiqliang@chinamobile.com](mailto:chengweiqliang@chinamobile.com)

### **Young Lee**

Sung Kyun Kwan University

Email: [younglee.tx@gmail.com](mailto:younglee.tx@gmail.com)

## **Адреса авторов**

### **Qin Wu** (editor)

Huawei  
101 Software Avenue  
Yuhua District  
Nanjing  
Jiangsu, 210012  
China  
Email: [bill.wu@huawei.com](mailto:bill.wu@huawei.com)

### **Mohamed Boucadair** (editor)

Orange  
Rennes 35000  
France  
Email: [mohamed.boucadair@orange.com](mailto:mohamed.boucadair@orange.com)

### **Diego R. Lopez**

Telefonica I+D  
Spain  
Email: [diego.r.lopez@telefonica.com](mailto:diego.r.lopez@telefonica.com)

### **Chongfeng Xie**

China Telecom  
Beijing  
China  
Email: [xiechf@chinatelecom.cn](mailto:xiechf@chinatelecom.cn)

### **Liang Geng**

China Mobile  
Email: [gengliang@chinamobile.com](mailto:gengliang@chinamobile.com)

## **Перевод на русский язык**

Николай Малых

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