Internet Engineering Task Force (IETF)
Request for Comments: 9408
Category: Standards Track
ISSN: 2070-1721

M. Boucadair, Ed.
Orange
O. Gonzalez de Dios
Telefonica
S. Barguil
Nokia
Q. Wu
Huawei
V. Lopez
Nokia

June 2023

A YANG Network Data Model for Service Attachment Points (SAPs)

Модель данных YANG для точек присоединения к сервису (SAP)

Аннотация

Этот документ определяет модель данных YANG для абстрактного представления топологии сети провайдера, содержащей точки, где можно подключиться к услугам (например, базовые соединения, VPN, сетевые срезы). Модель может также служить для извлечения точек, где услуги фактически предоставляются клиентам (включая сети партнёров).

Этот документ дополняет модель данных ietf-network из RFC 8345, добавляя в неё концепцию точек подключения к сервису (Service Attachment Point или SAP). SAP - это опорная точка сети, к которой могут подключаться сетевые услуги, такие как виртуальные частные сети сетевого (Layer 3 Virtual Private Network или L3VPN) и канального (Layer 2 Virtual Private Network или L2VPN) уровня. К одной точке SAP может быть привязана 1 или несколько служб. В модели данных SAP поддерживаются интерфейсы между пользователем и сетью (User-to-Network Interface или UNI) и между сетями (Network-to-Network Interface или NNI).

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.

Информация о текущем статусе документа, найденных ошибках и способах обратной связи доступна по ссылке https://www.rfc-editor.org/info/rfc9408.

Оглавление

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

1. Введение

Сервис-провайдеры предлагают своим клиентам множество сетевых услуг, включая виртуальные частные сети (Virtual Private Network или VPN), программно определяемые распределенные сети (Software-Defined Wide-Area Network или SD-WAN) с наложением [BGP-SDWAN-USAGE] и сетевые срезы (slice) [IETF-NETWORK-SLICES]. Для рационализации общих операций и повышения уровня автоматизации процедур предоставления услуг сервис-провайдерам нужно поддерживать представления о местах возможного доступа клиентов к услугам. Такое представление может служить, например, для обеспечения данными подразделения, отвечающего за обработку заказов на обслуживание, проверку доступности услуг, отслеживание охвата по услугам и т. п. (см., например, параграф 3.2 в [RFC8969]). Для этого в данном документе вводится концепция точек присоединения к сервису (Service Attachment Point или SAP).

SAP представляют собой опорные точки сети, где сетевые услуги могут быть предоставлены клиентам. Например, эта концепция служит для принятия решений о точках присоединения и предоставления услуг в модели услуг виртуальной частной сети на сетевом (Layer 3 VPN Service Model или L3SM) [RFC8299] или канальном (Layer 2 VPN Service Model (L2SM) [RFC8466] уровне. Она может также применяться для нахождения точек предоставления услуг клиентам по конфигурации сети, описанной в моделях сетевого (Layer 3 VPN Network Model или L3NM) [RFC9182] и канального (Layer 2 VPN Network Model или L2NM) [RFC9291] уровня.

Этот документ определяет сетевую модель YANG (6. Модуль YANG SAP) для представления, управления и контроля SAP. Модель дополняет в модуль ietf-network [RFC8345] концепцию SAP. В разделе 3. Пример использования сетевой модели SAP представлен пример использования модели. Этот документ разъясняет назначение и область действия сетевой модели SAP, а также её связь с другими моделями (4. Связи с другими моделями данных YANG).

Сеть может поддерживать несколько услуг, возможно разных типов. Предназначение топологии SAP для услуг определённого типа, отдельной услуги или набора разнотипных услуг зависит от развёртывания. Этот документ поддерживает все такие схемы внедрения.

В документе не применяются какие-либо допущения об услугах, предоставляемых сетью её пользователям. Службы VPN (например, L3VPN[1] или L2VPN[2]) [RFC4026] применяются в качестве иллюстраций (см. приложения A и B).

С учётом того, что интерфейсы между пользователем и сетью (User-to-Network Interface или UNI) и между сетями (Network-to-Network Interface или NNI) широко используются операторами для указания точек раздела при предоставлении услуг, этот документ поддерживает UNI SAP и NNI SAP. Примеры использования опорных точек UNI и NNI даны в [MEF6], [MEF17], [RFC6004], [RFC6215], для NNI в контексте VPN - в Приложении C.

Модель данных YANG в разделе 6 соответствует архитектуре хранилищ данных управления сетью (Network Management Datastore Architecture или NMDA) [RFC8342].

2. Терминология

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.

В документе предполагается знание читателем концепций [RFC6241], [RFC7950], [RFC8345], [RFC8309], поскольку в документе применяются термины из этих RFC.

В этом документе применяется графическое представление деревьев данных, определённое в [RFC8340].

Термин «модель сети» (network model) здесь применяется в соответствии с определением в параграфе 2.1 [RFC8969].

Ниже приведены определения используемых в документе терминов.

Service provider - поставщик услуг, сервис-провайдер
: Организация, отвечающая за работу сети, предоставляющей клиентам услуги (например, VPN).

Attachment Circuit (AC) - устройство присоединения
: Канал, соединяющий краевое устройство клиента (Customer Edge или CE) с краевым устройством провайдера (Provider Edge или PE).

Customer Edge (CE) - краевое устройство клиента
: Оборудование, предоставленное отдельному клиенту и напрямую соединённое с одним или несколькими PE через AC. Устройства CE обычно размещаются у клиента. CE может применяться для одной услуги (например, L3VPN), хотя может поддерживаться и несколько VPN, если они имеют отдельные AC. В качестве CE может служить маршрутизатор, мост, коммутатор и т. п.

Provider Edge (PE) - краевое устройство провайдера
: Принадлежащее провайдеру и управляемое им оборудование, которое может поддерживать множество услуг (например, VPN) для разных клиентов. PE напрямую соединяется с одним или несколькими CE через AC.

Service Attachment Points (SAPs) - точки присоединения к сервису
: Абстракция опорных точек сети (например, обращённая к PE сторона AC или обращённая к CE сторона AC при управлении CE со стороны провайдера), где сетевые услуги предоставляются или могут предоставляться клиентам. Точка SAP может связана с одним или несколькими AC.

3. Пример использования сетевой модели SAP

Операции управления у сервис-провайдера могут быть автоматизированы с использованием разных способов, таких как интерфейсы на основе модулей YANG [RFC8969] [RFC6241] [RFC8040]. С этой точки зрения и с учётом архитектуры, показанной на рисунке 1, целью этого документа является предоставление механизма на основе интерфейса YANG для отображения абстрактного представления сети от сетевого контроллера до уровня организации обслуживания с упором на точки предоставления услуг клиентам. Модель также служит для отыскания опорных точек сети, где услуги будут предоставляться клиентам. Для услуг, которым нужны ресурсы партнерских сетей модель также служит для раскрытия NNI.

[1] Layer 3 Virtual Private Network - виртуальная частная сеть на сетевом уровне.
[2] Layer 2 Virtual Private Network - виртуальная частная сеть на канальном уровне.

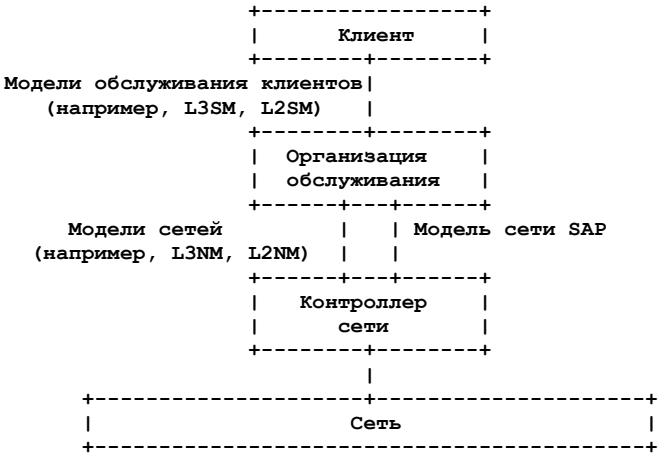

Рисунок 1. Использование модели SAP.

В разделе 5 [RFC4026] приведён обзор блоков, которые обычно применяются для классификации сетей провайдеров.

Уровню организации (orchestration) сервиса не требуется знать детали устройства базовой сети (например, узлы P, см. параграф 5.3.1 в [RFC4026])). На рисунке 2 приведено абстрактное представление сети с точки зрения организатора услуг. Однако этого представления недостаточно для предоставления уровню организации сервиса сведений для создания сетевых услуг. Топология сервиса должна обеспечивать возможность раскрыть набор узлов и связанные с ними точки присоединения, где могут быть предоставлены сетевые услуги.

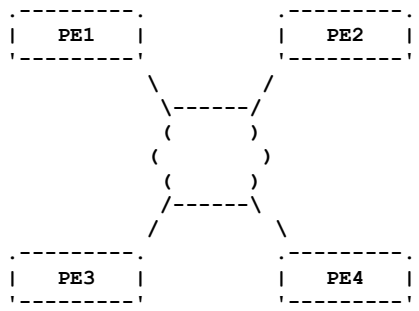

Рисунок 2. Абстрактная топология сети.

Как правило, уровень организации обслуживания, ориентируясь на UNI, будет видеть набор PE и интерфейсов (физических или логических) в сторону клиентов, к которым могут подключаться (или уже подключены) CE. Такие интерфейсы также называют UNI-N[1] [RFC6215]. Уровень организации обслуживания может использовать такие интерфейсы для организации или предоставления запрошенных услуг. На рисунке 3 дан пример сетевой топологии SAP, которая поддерживается контроллером сети и раскрывается оркестратору служб.

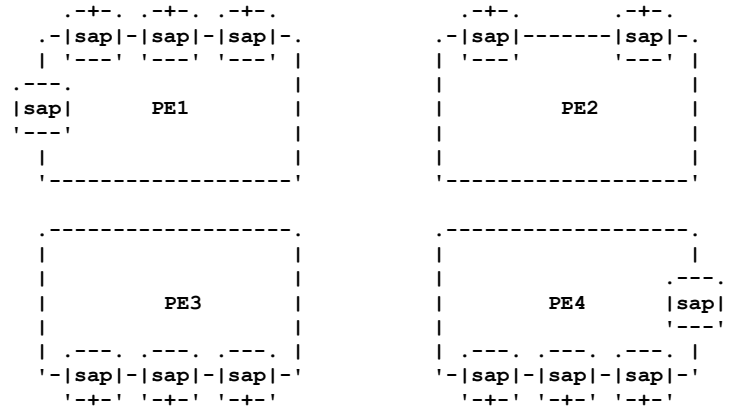

Рисунок 3. Сетевая топология SAP.

Отдельная топология сети SAP может применяться для организации одного или нескольких типов услуг (например, L3VPN, Ethernet VPN - EVPN)). Контроллер сети может раскрывать типы услуг и связанными с ними интерфейсы через SAP.

Как показано на рисунке 4, уровень организации услуг будет иметь доступ к набору моделей обслуживания клиентов (например, L3SM или L2SM) на интерфейсах в сторону клиентов и набору моделей сетей (например, L3NM и модели данных топологии сети) на интерфейсах в сторону ресурсов. В таких случаях предполагается, что контроллер не знает о происходящем за PE в направлении CE и отвечает только за управление и контроль точек SAP и сетей между PE. Для сопоставления точек доставки из запросов услуг и SAP модель SAP может включать идентификатор партнерской точки (CE, сайта и т. п.).

[1]User-to-Network Interface, Network side - сетевая сторона интерфейса между пользователем и сетью.

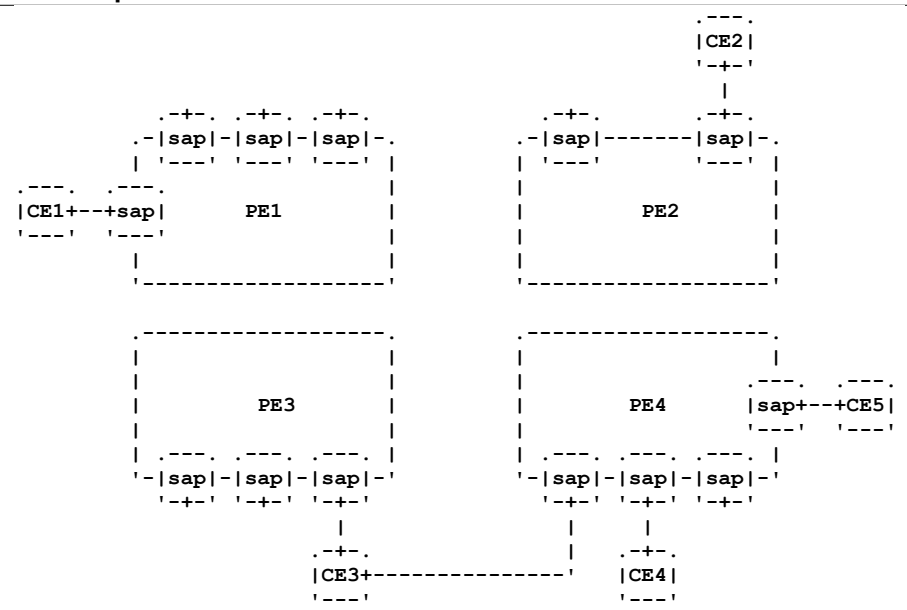

Рисунок 4. Топология сети с CE и AC.

В Приложении A приведён пример, отражающий топологию, показанную на рисунке 4.

4. Связи с другими моделями данных YANG

Модель сети SAP можно рассматривать как данные инвентаризации, связанные с точками SAP. Модель поддерживает опись обращённых к клиентам устройств в сети, основанной на [RFC8345]. На рисунке 5 показаны связи сетевой модели SAP с другими моделями. Модель сети SAP дополняет модель сети из [RFC8345] и импортирует модель топологии сети из [RFC8345], а другие модели топологии, связанные с конкретной технологией (например, модель топологии TE[1] [RFC8795] или топологии L3 [RFC8346]) дополняют модель топологии сети из [RFC8345].

Рисунок 5. Связь модели сети SAP с другими моделями.

SAP можно рассматривать как обращённые к клиенту точки завершения (termination point или TP) с предоставлением конкретных услуг. Различие между SAP и TP состоит в том, что канал завершается одной точкой TP (параграф 4.4.6 в [RFC8345]), тогда как AC может завершаться несколькими SAP. Кроме того, SAP не является точкой завершения туннеля (tunnel termination point или TTP, см. параграф 3.6 в [RFC8795]) или канала.

В контексте программно определяемых сетей (Software-Defined Networking или SDN) [RFC7149] [RFC7426] модель данных YANG SAP можно применять для обмена сведениями между элементами управления, чтобы поддерживать предоставление услуг VPN и управление ресурсами в соответствии с [RFC9182] и [RFC9291]. С помощью этой модели данных уровень организации услуг может узнать о доступных конечных точках (SAP) соединительных ресурсов базовой сети. Уровень организации обслуживания может определить конечные точки соединений для добавления в сервис L2VPN или L3VPN. С помощью других моделей данных (например, L3SM [RFC8299] или L2SM [RFC8466]) иерархические элементы управления могут оценить доступность сквозной связности IP или связности L2VPN и, следовательно, определить последовательность доменов и соединительных точек для использования.

Связанные с интерфейсами расширенные узлы данных не включены в модель SAP. Указанные в этой модели идентификаторы интерфейсов используются в качестве фильтров для установки или извлечения данные с использованием моделей данных устройств (например, [RFC7224]).

5. Дерево модуля SAP

Модель данных сети SAP ietf-sap-ntw создана на основе модуля ietf-network [RFC8345], дополненного узлами с SAP.

Структура модуля ietf-sap-ntw показана на рисунке 6.

[1]Traffic Engineering - организация (построение) трафика.

```
module: ietf-sap-ntw
  augment /nw:networks/nw:network/nw:network-types:
    +--rw sap-network!
       +--rw service-type*   identityref
  augment /nw:networks/nw:network/nw:node:
    +--rw service* [service-type]
       +--rw service-type                    identityref
       +--rw sap* [sap-id]
          +--rw sap-id                       string
          +--rw description?                 string
          +--rw parent-termination-point?    nt:tp-id
          +--rw attachment-interface?        string
          +--rw interface-type?              identityref
          +--rw encapsulation-type?          identityref
          +--rw role?                        identityref
          +--rw allows-child-saps?           boolean
          +--rw peer-sap-id*                 string
          +--ro sap-status
          |  +--ro status?         identityref
          |  +--ro last-change?    yang:date-and-time
          +--rw service-status
             +--rw admin-status
             |  +--rw status?         identityref
             |  +--rw last-change?    yang:date-and-time
             +--ro oper-status
                +--ro status?         identityref
                +--ro last-change?    yang:date-and-time
```

Рисунок 6. Структура дерева модуля YANG SAP.

Топология сети SAP может служить для предоставления 1 или нескольких типов услуг (service-type). Примеры поддерживаемых типов услуг приведены ниже.

- L3VPN [RFC4364];
- виртуальные частные ЛВС (Virtual Private LAN Service или VPLS) [RFC4761] [RFC4762];
- Виртуальные частные линии (Virtual Private Wire Service или VPWS) [RFC8214];
- Ethernet VPN на основе BGP MPLS [RFC7432];
- VPWS в Ethernet VPN [RFC8214];
- Магистральные мосты провайдера (Provider Backbone Bridging) в сочетании с Ethernet VPN (PBB-EVPN) [RFC7623]
- EVPN на основе VXLAN[1] [RFC8365];
- виртуальные сети [RFC8453];
- расширенные VPN (VPN+) [ENHANCED-VPN];
- сетевые «срезы» (slice) [IETF-NETWORK-SLICES];
- SD-WAN [BGP-SDWAN-USAGE];
- базовая связность IP.

Эти типы услуг создаются на основе типов, уже заданных в [RFC9181], и дополнительных типов, определённых здесь. В будущих модулях YANG (включая пересмотр заданного здесь модуля YANG) при необходимости могут быть определены новые типы услуг.

> Применение типов услуг, заданных в [RFC9181] означает упрощение сопоставления топологии SAP и соответствующих моделей сетей, которые применяются для предоставления конкретных услуг через сети провайдеров.

Для доступа к топологии SAP в соответствии с услугами могут применяться фильтры по типам услуг. Пример этого показан на рисунке 10 в Приложении B.

Узел в топологии может поддерживать 1 или несколько типов услуг (service-type) из числа перечисленных в контейнере sap-network. Затем к каждому типу услуг привязывается список SAP, поддерживающих этот тип. Характеристики SAP приведены ниже.

sap-id

Идентификатор, однозначно указывающий SAP в рамках узла.
Одна точка SAP может присутствовать в разных типах услуг и в таком случае все они используют общий идентификатор SAP.
SAP, связанные с интерфейсами, где непосредственно размещаются службы, интерфейсы, которые готовы поддерживать субинтерфейсы для служб (ещё не активированные), или службы, уже созданные на субинтерфейсах, указываются в качестве SAP. На рисунке 9 в Приложении B показано, как можно указать службы, способные размещать субинтерфейсы по службам.
Например, sap-id может быть идентификатором сети VPN, как определено в параграфе 7.6 [RFC9182]. Пример, иллюстрирующий применение этого атрибута при создании сервиса, представлен в Приложении D.

description

Текстовое описание SAP.

[1]Virtual eXtensible Local Area Network - виртуальная расширяемая ЛВС.

parent-termination-point

Ссылка на родительскую точку завершения, с которой связана точка SAP. В соответствии с параграфом 4.2 в [RFC8345] точка завершения служит окончанием канала на узле и может быть физическим портом, интерфейсом и т. п. Указанная родительская точка завершения предполагается обращённой в сторону клиента, а не ядра сети.

Этот атрибут может применяться, например, для связывания интерфейса с субинтерфейсами, поскольку все они могут быть указаны как SAP узла. Атрибут служит также для связывания SAP с физической топологией.

Этот узел может применяться, например, для отображения конечных точек IETF Network Slice [IETF-NETWORK-SLICES] на конечные точки служб/туннелей/путей в базовой сети.

attachment-interface

Ссылка на интерфейс, с которым связана точка SAP. Один интерфейс может поддерживать несколько служб. В зависимости от развёртывания идентификатор присоединения может отражать интерфейс соединения.

Например, этой ссылкой может служить любой из идентификаторов (l2-termination-point, local-bridge-reference, bearer-reference, lag-interface-id), определённых в параграфе 7.6.1 [RFC9182] или l3-termination-point, определённый в параграфе 7.6.2 [RFC9182]. Контроллер отвечает за обеспечение использования согласованных ссылок в SAP и моделях базовых устройств или иных механизмах инвентаризации устройств.

interface-type

Указывает тип порта, к которому привязана точка SAP - физический порт, петлевой интерфейс (loopback(, интерфейс агрегированного канала (Link Aggregation Group или LAG) [IEEE802.1AX], интерфейс интегрированной с мостом маршрутизации (Integrated Routing and Bridging или IRB) (например, [RFC9135]), интерфейс локального моста и т. п..

Сопоставление с конкретными типами интерфейсом в соответствии с [RFC7224] поддерживает контролёр. Это сопоставление применяется, например, при трансляции контроллером сетевой модели SAP в модели устройств (параграф 4.4 в [RFC8969]).

encapsulation-type

Тип инкапсуляции для интерфейса, указанного атрибутом attachment-interface (см. [RFC9181]). Этот узел данных применяется, например, для решения вопроса о возможности многократного использования имеющейся точки SAP для поддержки сервиса или создания нового субинтерфейса.

role

Указывает роль SAP (например, UNI или NNI). SAP наследует роль родительского интерфейса (parent- termination-point).

allows-child-saps

Значение true указывает, что интерфейс присоединения для этой точки SAP может поддерживать субинтерфейсы для служб. Возможность прямого присоединения к родительской точке SAP в дополнение к дочерним SAP зависит от службы.

peer-sap-id

Ссылки на удалённые точки AC. Этот идентификатор может (но не обязан) совпадать с идентификатором SAP, используемым в конфигурации партнёра. Использование идентичных идентификаторов упрощает сопоставление между запросом на обслуживание партнёра и локальной точкой SAP. Примерами таких ссылок являются идентификаторы сайтов (параграф 6.3 в [RFC8299]), точек разделения служб (Service Demarcation Point или SDP, см. параграф 3.2 в [IETF-NETWORK-SLICES]) и адреса IP граничных маршрутизаторов партнерских автономных систем (Autonomous System Border Router или ASBR).

sap-status

Указывает рабочее состояние SAP, значения состояний определены в [RFC9181].

Когда присутствует родительский интерфейс и субинтерфейс, но родительский интерфейс отключён, статус этого интерфейса имеет предпочтение перед статусом, указанным субинтерфесом.

service-status

Указывает административное и рабочее состояние для данной точки SAP. Эти сведения особенно полезны, когда одна точка SAP обеспечивает несколько служб, из которых активна лишь часть. Поэтому рабочему значению sap-status **недопустимо** влиять на административное значение service-status.

Значение oper-status для службы указывает её рабочее состояние, наблюдаемое в конкретной точке SAP, а не статус службы в масштабе сети с множеством SAP. Статус службы в масштабе сети можно определить с использованием соответствующей модели сети, например из числа указанных в параграфе 7.3 [RFC9182] или параграфе 7.3 [RFC9291].

Для оценки статуса предоставления услуг в данной точке SAP рекомендуется проверять административное и рабочее состояние (service-status) в дополение к sap-status. При этом контроллер сети (или оператор) может обнаруживать аномалии. Например, если служба административно включена для SAP, а sap-status для этой точки SAP указывает отключения (down), предполагается, что oper-status также указывает отключение (down). Отдельное получение рабочего состояния в таких условиях может применяться для обнаружения аномалий. Аналогичным способом можно сравнить административное и рабочее состояние для обнаружения относящихся к службе аномалий активации SAP. Например, активное рабочее состояние SAP для службы, объявленной неактивной для SAP административно, говорит о необходимости приведения наблюдаемого состояния службы с ожидаемым.

6. Модуль YANG SAP

Этот модуль импортирует типы из [RFC6991], [RFC8345], [RFC9181]. Узлы sap-entry и sap-list определены как группировки (grouping) для их использования в модулях YANG конкретных служб.

```
<CODE BEGINS> file "ietf-sap-ntw@2023-06-20.yang"
module ietf-sap-ntw {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-sap-ntw";
  prefix sap;

  import ietf-network-topology {
    prefix nt;
    reference
      "RFC 8345: A YANG Data Model for Network
                 Topologies, Section 6.2";
  }
  import ietf-network {
```

```
    prefix nw;
    reference
      "RFC 8345: A YANG Data Model for Network
                 Topologies, Section 6.1";
  }
  import ietf-vpn-common {
    prefix vpn-common;
    reference
      "RFC 9181: A Common YANG Data Model for Layer 2 and Layer 3
                 VPNs";
  }
  import ietf-yang-types {
    prefix yang;
    reference
      "RFC 6991: Common YANG Data Types, Section 3";
  }

  organization
    "IETF OPSA (Operations and Management Area) Working Group";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/opsawg/>
     WG List:  <mailto:opsawg@ietf.org>

     Editor:   Mohamed Boucadair
               <mailto:mohamed.boucadair@orange.com>

     Author:   Oscar Gonzalez de Dios
               <mailto:oscar.gonzalezdedios@telefonica.com>

     Author:   Samier Barguil
               <mailto:samier.barguil_giraldo@nokia.com>

     Author:   Qin Wu
               <mailto:bill.wu@huawei.com>

     Author:   Victor Lopez
               <mailto:victor.lopez@nokia.com>";
  description
    "Этот модуль YANG задаёт модель для представления, управления и
     контроля точек доступа к сервису (SAP) в сетевой топологии.

     Авторские права (Copyright (c) 2023) 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 9408, где правовые
     аспекты приведены более полно.";

  revision 2023-06-20 {
    description
      "Initial version.";
    reference
      "RFC 9408: A YANG Network Data Model for Service Attachment
                 Points (SAPs)";
  }

  identity virtual-network {
    base vpn-common:service-type;
    description
      "Виртуальная сеть - экземпляр логической сети, созданный
       на основе физической сети.";
    reference
      "RFC 8453: Framework for Abstraction and Control of TE
                 Networks (ACTN)";
  }

  identity enhanced-vpn {
    base vpn-common:service-type;
    description
      "расширенная VPN (VPN+). Подход VPN+ основан на имеющихся
       технологиях VPN и TE с добавлением характеристик, нужных
       конкретным службам, в дополнение к традиционным VPN.";
    reference
      "draft-ietf-teas-enhanced-vpn:
         A Framework for Enhanced Virtual Private Network
         (VPN+)";
  }

  identity network-slice {
    base vpn-common:service-type;
    description
```

```
        "IETF Network Slice - топология логической сети, соединяющая
         множество конечных точек с использованием набора общих
         или выделенных сетевых ресурсов, служащих для достижения
         целей конкретной службы.";
      reference
        "draft-ietf-teas-ietf-network-slices:
           A Framework for IETF Network Slices";
    }

    identity sdwan {
      base vpn-common:service-type;
      description
        "Программно определяемая распределенная сеть (SD-WAN)
         на основе PE.";
      reference
        "draft-ietf-bess-bgp-sdwan-usage:
           BGP Usage for SD-WAN Overlay Networks";
    }

    identity basic-connectivity {
      base vpn-common:service-type;
      description
        "Базовая связность IP, например, «плоская» связность,
         обеспечиваемая для организаций через общую или выделенную
         инфраструктуру MPLS.";
    }

    identity interface-role {
      description
        "Базовый идентификатор роли интерфейса в сети.";
    }

    identity uni {
      base interface-role;
      description
        "Интерфейс между пользователем и сетью (UNI).";
    }

    identity nni {
      base interface-role;
      description
        "Интерфейс между сетями (NNI).";
    }

    identity interface-type {
      description
        "Базовый идентификатор для типа интерфейса.";
    }

    identity phy {
      base interface-type;
      description
        "Физический порт.";
    }

    identity loopback {
      base interface-type;
      description
        "Петлевой (loopback) интерфейс.";
    }

    identity lag {
      base interface-type;
      description
        "Интерфейс композитного канала (LAG).";
    }

    identity irb {
      base interface-type;
      description
        "Интерфейс интегрированного с маршрутизацией моста (IRB). Такие
         интерфейсы обычно соединяют элементы виртуальной маршрутизации
         и пересылки IP (IP-VRF) с доменом моста.";
    }

    identity local-bridge {
      base interface-type;
      description
        "Ссылка на локальный мост для размещения, например, реализаций,
         которым нужен внутренний мост. При использовании такого типа
         для идентификации интерфейса служит ссылка на локальный домен
         моста.";
    }

    identity logical {
      base interface-type;
```

```
      description
        "Указывает локальный интерфейс, который обычно служит для
         привязки сервиса. Этот тип применяется лишь при невозможности
         использовать более конкретный тип (loopback, lag, irb,
         local-bridge).";
    }

    grouping sap-entry {
      description
        "Сведения о точке присоединения к службе (SAP).";
      leaf sap-id {
        type string;
        description
          "Идентификатор, однозначно указывающий SAP.";
      }
      leaf description {
        type string;
        description
          "Текстовое описание SAP.";
      }
      leaf parent-termination-point {
        type nt:tp-id;
        description
          "Указывает родительскую точку завершения, к которой
           присоединена точка SAP. Это может быть физический порт,
           интерфейс и т. п.";
      }
      leaf attachment-interface {
        type string;
        description
          "Интерфейс, к которому привязана точка SAP.";
      }
      leaf interface-type {
        type identityref {
          base interface-type;
        }
        description
          "Тип интерфейса, к которому привязана точка SAP.";
      }
      leaf encapsulation-type {
        type identityref {
          base vpn-common:encapsulation-type;
        }
        description
          "Тип инкапсуляции интерфейса, к которому привязана
           точка SAP.";
      }
      leaf role {
        type identityref {
          base interface-role;
        }
        description
          "Указывает роль SAP.";
      }
      leaf allows-child-saps {
        type boolean;
        description
          "Указывает, способен ли интерфейс этой точки SAP поддерживать
           субинтерфейсы для служб.";
      }
      leaf-list peer-sap-id {
        type string;
        description
          "Указывает идентификатор точки завершения партнёра (например,
           CE). Эти сведения могут служить для сопоставления, такого
           как идентификация точки SAP, подключённой к конечной точке,
           указанной в запросе сервиса.";
      }
    }

    grouping sap-list {
      description
        "Сведения о SAP.";
      list sap {
        key "sap-id";
        description
          "SAP является обстракцией точки, с которой могут быть связаны
           сетевые службы, такие как L3VPN, L2VPN, сетевые срезы.";
        uses sap-entry;
        container sap-status {
          config false;
          description
            "Указывает рабочее состояние SAP независимо от
             предоставляемых через эту точку услуг.";

          uses vpn-common:oper-status-timestamp;
```

```
        }
        container service-status {
          description
            "Указывает статус сервиса.";
          container admin-status {
            description
              "Административный статус сервиса.";
            leaf status {
              type identityref {
                base vpn-common:administrative-status;
              }
              description
                "Административный статус сервиса, предоставляемого
                 в SAP.";
            }
            leaf last-change {
              type yang:date-and-time;
              description
                "Фактическая дата и время смены статуса сервиса.";
            }
          }
          container oper-status {
            config false;
            description
              "Рабочий статус сервиса, предоставляемого в SAP.";
            uses vpn-common:oper-status-timestamp;
          }
        }
      }
    }

    augment "/nw:networks/nw:network/nw:network-types" {
      description
        "Новый тип сети для сети SAP.";
      container sap-network {
        presence "Указывает тип сети SAP.";
        description
          "Наличие контейнера указывает сеть SAP.";
        leaf-list service-type {
          type identityref {
            base vpn-common:service-type;
          }
          description
            "Указывает набор поддерживаемых типов услуг.";
        }
      }
    }

    augment "/nw:networks/nw:network/nw:node" {
      when '../nw:network-types/sap:sap-network' {
        description
          "Параметры дополнения, применяемые лишь к сети SAP.";
      }
      description
        "Параметры SAP на уровне узла.";
      list service {
        key "service-type";
        description
          "Список поддерживаемых узлом типов услуг.";
        leaf service-type {
          type identityref {
            base vpn-common:service-type;
          }
          description
            "Тип сервиса.";
        }
        uses sap-list;
      }
    }
  }
  <CODE ENDS>
```

7. Взаимодействие с IANA

Этот документ регистрирует URI в субреестре ns реестра IETF XML Registry [RFC3688].

```
URI:  urn:ietf:params:xml:ns:yang:ietf-sap-ntw
Registrant Contact:  The IESG.
XML:  N/A; запрошенный URI является пространством имён XML.
```

Документ регистрирует модуль YANG в суб реестре YANG Module Names [RFC6020] реестра YANG Parameters.

```
Name:  ietf-sap-ntw
Namespace:  urn:ietf:params:xml:ns:yang:ietf-sap-ntw
Maintained by IANA?  N
Prefix:  sap
Reference:  RFC 9408
```

8. Вопросы безопасности

Заданный этим документом модуль YANG определяет схему для данных, предназначенную для доступа через сеть с использованием протоколов управления, таких 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 доступа к конфигурации сети (NACM – Network Configuration Access Control Model) [RFC8341] обеспечивает возможность разрешить доступ лишь определённых пользователей NETCONF или RESTCONF к заранее заданному подмножеству операций NETCONF или RESTCONF и содержимого.

В заданном здесь модуле данных YANG определено множество узлов данных, которые разрешают запись, создание и удаление (т. е. config true, как принято по умолчанию). Эти узлы могут быть конфиденциальными или уязвимыми в некоторых сетевых средах. Запись в такие узлы (например, edit-config) без должной защиты может негативно влиять на работу сети. Ниже перечислены ветви и узлы, которые могут быть конфиденциальны или уязвимы.

/nw:networks/nw:network/nw:node/sap:service/sap:sap

Эта ветвь задаёт конфигурацию узлов в модели сети SAP. Неожиданные изменения в ветви (например, связывание SAP с другой родительской точкой завершения) могут приводить к нарушению работы службы и/или некорректному поведению сети. Некорректное поведение возникает главным образом из-за конфигурации сети, не соответствующей предполагаемому оператором поведению (см., например, параграф 4.2.1 в [RFC8969]).

Некоторые из доступных для чтения узлов в этом модуле YANG могут быть конфиденциальны или уязвимы в той или иной сетевой среде. Важно контролировать доступ к таким объектам (например, get, get-config, notification). Ниже перечислены ветви и узлы, которые могут быть конфиденциальны или уязвимы.

/nw:networks/nw:network/nw:node/sap:service/sap:sap

Несанкционированный доступ к этой ветви может раскрывать сведения о рабочем состоянии узлов в модели сети SAP (например, отождествление клиента в peer-sap-id).

9. Литература

9.1. 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>.

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

[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>.

[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>.

[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., Ananthakrishnan, 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>.

[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>.

[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>.

[RFC9181] Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., and Q. Wu, "A Common YANG Data Model for Layer 2 and Layer 3 VPNs", RFC 9181, DOI 10.17487/RFC9181, February 2022, <https://www.rfc-editor.org/info/rfc9181>.

9.2. Дополнительная литература

[BGP-SDWAN-USAGE] Dunbar, L., Guichard, J., Sajassi, A., Drake, J., Najem, B., Banerjee, A., and D. Carrel, "BGP Usage for SD-WAN Overlay Networks", Work in Progress, Internet-Draft, draft-ietf-bess-bgp-sdwan-usage-09, 7 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-bess-bgp-sdwan-usage-09>.

[ENHANCED-VPN] Dong, J., Bryant, S., Li, Z., Miyasaka, T., and Y. Lee, "A Framework for Enhanced Virtual Private Network (VPN+)", Work in Progress, Internet-Draft, draft-ietf-teas-enhanced-vpn-12, 23 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-enhanced-vpn-12>.

[IEEE802.1AX] IEEE, "IEEE Standard for Local and Metropolitan Area Networks--Link Aggregation", IEEE Std 802.1AX-2020, DOI 10.1109/IEEESTD.2020.9105034, 2020, <https://doi.org/10.1109/IEEESTD.2020.9105034>.

[IETF-NETWORK-SLICES] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L.M., and J. Tantsura, "A Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-19, 21 January 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-19>.

[MEF17] The Metro Ethernet Forum, "Technical Specification MEF 17, Service OAM Requirements & Framework - Phase 1", April 2007, <https://www.mef.net/wp-content/uploads/2015/04/MEF-17.pdf>.

[MEF6] The Metro Ethernet Forum, "Technical Specification MEF 6, Ethernet Services Definitions - Phase I", June 2004, <https://www.mef.net/Assets/Technical_Specifications/PDF/MEF_6.pdf>.

[RFC4026] Andersson, L. and T. Madsen, "Provider Provisioned Virtual Private Network (VPN) Terminology", RFC 4026, DOI 10.17487/RFC4026, March 2005, <https://www.rfc-editor.org/info/rfc4026>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[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>.

[RFC6004] Berger, L. and D. Fedyk, "Generalized MPLS (GMPLS) Support for Metro Ethernet Forum and G.8011 Ethernet Service Switching", RFC 6004, DOI 10.17487/RFC6004, October 2010, <https://www.rfc-editor.org/info/rfc6004>.

[RFC6215] Bocci, M., Levrau, L., and D. Frost, "MPLS Transport Profile User-to-Network and Network-to-Network Interfaces", RFC 6215, DOI 10.17487/RFC6215, April 2011, <https://www.rfc-editor.org/info/rfc6215>.

[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>.

[RFC7426] Haleplidis, E., Ed., Pentikousis, K., Ed., Denazis, S., Hadi Salim, J., Meyer, D., and O. Koufopavlou, "Software-Defined Networking (SDN): Layers and Architecture Terminology", RFC 7426, DOI 10.17487/RFC7426, January 2015, <https://www.rfc-editor.org/info/rfc7426>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

[RFC7623] Sajassi, A., Ed., Salam, S., Bitar, N., Isaac, A., and W. Henderickx, "Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)", RFC 7623, DOI 10.17487/RFC7623, September 2015, <https://www.rfc-editor.org/info/rfc7623>.

[RFC7951] Lhotka, L., "JSON Encoding of Data Modeled with YANG", RFC 7951, DOI 10.17487/RFC7951, August 2016, <https://www.rfc-editor.org/info/rfc7951>.

[RFC8214] Boutros, S., Sajassi, A., Salam, S., Drake, J., and J. Rabadan, "Virtual Private Wire Service Support in Ethernet VPN", RFC 8214, DOI 10.17487/RFC8214, August 2017, <https://www.rfc-editor.org/info/rfc8214>.

[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>.

[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>.

[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>.

[RFC8365] Sajassi, A., Ed., Drake, J., Ed., Bitar, N., Shekhar, R., Uttaro, J., and W. Henderickx, "A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)", RFC 8365, DOI 10.17487/RFC8365, March 2018, <https://www.rfc-editor.org/info/rfc8365>.

[RFC8453] Ceccarelli, D., Ed. and Y. Lee, Ed., "Framework for Abstraction and Control of TE Networks (ACTN)", RFC 8453, DOI 10.17487/RFC8453, August 2018, <https://www.rfc-editor.org/info/rfc8453>.

[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>.

[RFC8969] Wu, Q., Ed., Boucadair, M., Ed., Lopez, D., Xie, C., and L. Geng, "A Framework for Automating Service and Network Management with YANG", RFC 8969, DOI 10.17487/RFC8969, January 2021, <https://www.rfc-editor.org/info/rfc8969>.

[RFC9135] Sajassi, A., Salam, S., Thoria, S., Drake, J., and J. Rabadan, "Integrated Routing and Bridging in Ethernet VPN (EVPN)", RFC 9135, DOI 10.17487/RFC9135, October 2021, <https://www.rfc-editor.org/info/rfc9135>.

[RFC9182] Barguil, S., Gonzalez de Dios, O., Ed., Boucadair, M., Ed., Munoz, L., and A. Aguado, "A YANG Network Data Model for Layer 3 VPNs", RFC 9182, DOI 10.17487/RFC9182, February 2022, <https://www.rfc-editor.org/info/rfc9182>.

[RFC9291] Boucadair, M., Ed., Gonzalez de Dios, O., Ed., Barguil, S., and L. Munoz, "A YANG Network Data Model for Layer 2 VPNs", RFC 9291, DOI 10.17487/RFC9291, September 2022, <https://www.rfc-editor.org/info/rfc9291>.

Приложение A. Пример упрощённой сети SAP

На рисунке 7 показан пример топологии SAP, о которой сообщает контроллер сети. Этот пример отражает топологию, показанную на рисунке 4. Для каждой точки SAP представлен лишь минимальный набор сведений, в частности, не указаны узлы parent-termination-point, attachment-interface, interface-type, encapsulation-type, role. Точки SAP, способные предоставлять услуги, но ещё не активированные, указаны sap-status/status со значением ietf-vpn-common:op-down и service-status/admin-status/status со значением ietf-vpn-common:admin-down. SAP, где включено предоставление услуг указаны service-status/admin-status/status со значением ietf-vpn-common:admin-up и service-status/oper-status/status со значением ietf-vpn-common:op-up. Отметим, что указанные в разделе 5 аномалии не наблюдались для этих SAP. Тело сообщения на рисунка ниже представлено в кодировании JSON для данных YANG в соответствии с [RFC7951].

```
{
  "ietf-network:networks": {
    "network": [
      {
        "network-types": {
          "ietf-sap-ntw:sap-network": {
            "service-type": [
              "ietf-vpn-common:l3vpn",
              "ietf-vpn-common:vpls"
            ]
          }
        },
        "network-id": "example:an-id",
        "node": [
          {
            "node-id": "example:pe1",
            "ietf-sap-ntw:service": [
              {
                "service-type": "ietf-vpn-common:l3vpn",
                "sap": [
                  {
                    "sap-id": "sap#11",
                    "peer-sap-id": ["ce-1"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#12",
                    "sap-status": {
                      "status": "ietf-vpn-common:op-down"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-down"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#13",
                    "sap-status": {
                      "status": "ietf-vpn-common:op-down"
```

```
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-down"
              }
            }
          },
          {
            "sap-id": "sap#14",
            "sap-status": {
              "status": "ietf-vpn-common:op-down"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-down"
              }
            }
          }
        ]
      }
    ]
  },
  {
    "node-id": "example:pe2",
    "ietf-sap-ntw:service": [
      {
        "service-type": "ietf-vpn-common:l3vpn",
        "sap": [
          {
            "sap-id": "sap#21",
            "sap-status": {
              "status": "ietf-vpn-common:op-down"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-down"
              }
            }
          },
          {
            "sap-id": "sap#22",
            "peer-sap-id": ["ce-2"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-up"
              },
              "oper-status": {
                "status": "ietf-vpn-common:op-up"
              }
            }
          }
        ]
      }
    ]
  },
  {
    "node-id": "example:pe3",
    "ietf-sap-ntw:service": [
      {
        "service-type": "ietf-vpn-common:l3vpn",
        "sap": [
          {
            "sap-id": "sap#31",
            "sap-status": {
              "status": "ietf-vpn-common:op-down"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-down"
              }
            }
          },
          {
            "sap-id": "sap#32",
            "sap-status": {
              "status": "ietf-vpn-common:op-down"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-down"
              }
            }
          },
```

```
            {
              "sap-id": "sap#33",
              "peer-sap-id": ["ce-3"],
              "sap-status": {
                "status": "ietf-vpn-common:op-up"
              },
              "service-status": {
                "admin-status": {
                  "status": "ietf-vpn-common:admin-up"
                },
                "oper-status": {
                  "status": "ietf-vpn-common:op-up"
                }
              }
            }
          ]
        }
      ]
    },
    {
      "node-id": "example:pe4",
      "ietf-sap-ntw:service": [
        {
          "service-type": "ietf-vpn-common:l3vpn",
          "sap": [
            {
              "sap-id": "sap#41",
              "peer-sap-id": ["ce-3"],
              "sap-status": {
                "status": "ietf-vpn-common:op-up"
              },
              "service-status": {
                "admin-status": {
                  "status": "ietf-vpn-common:admin-up"
                },
                "oper-status": {
                  "status": "ietf-vpn-common:op-up"
                }
              }
            },
            {
              "sap-id": "sap#42",
              "peer-sap-id": ["ce-4"],
              "sap-status": {
                "status": "ietf-vpn-common:op-up"
              },
              "service-status": {
                "admin-status": {
                  "status": "ietf-vpn-common:admin-up"
                },
                "oper-status": {
                  "status": "ietf-vpn-common:op-up"
                }
              }
            },
            {
              "sap-id": "sap#43",
              "sap-status": {
                "status": "ietf-vpn-common:op-down"
              },
              "service-status": {
                "admin-status": {
                  "status": "ietf-vpn-common:admin-down"
                }
              }
            },
            {
              "sap-id": "sap#44",
              "peer-sap-id": ["ce-5"],
              "sap-status": {
                "status": "ietf-vpn-common:op-up"
              },
              "service-status": {
                "admin-status": {
                  "status": "ietf-vpn-common:admin-up"
                },
                "oper-status": {
                  "status": "ietf-vpn-common:op-up"
                }
              }
            }
          ]
        }
      ]
    }
  ]
```

```
        }
      ]
    }
  }
```

Рисунок 7. Пример упрощённой модели SAP.

Приложение B. Простой пример модели SAP - фильтр узлов

В примере на рисунке 8 PE1 (с node-id example:pe1, как показано на рисунке 7) имеет 2 физических интерфейса GE0/6/1 и GE0/6/4. Два субинтерфейса GE0/6/4.1 и GE0/6/4.2 связаны с физическим интерфейсом GE0/6/4. Представим, что организатору обслуживания раскрываются 4 SAP, сопоставленные с этими физическими интерфейсами и их субинтерфейсами.

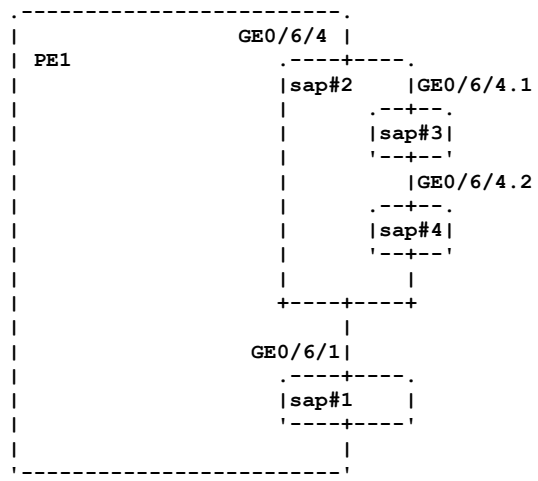

Рисунок 8. Пример PE и его интерфейсов.

Предположим, что для точки SAP, связанной с физическим интерфейсом GE0/6/1, сервис ещё не включён, а для SAP, связанных с физическим интерфейсом GE0/6/4, активированы службы VPLS и L3VPN на субинтерфейсах GE0/6/4.1 и GE0/6/4.2, соответственно. Точки sap#1 и sap#2 помечены как способные поддерживать службы на субинтерфейсах (allows-child-saps true).

Организатор служб может запросить у контроллера сети, например, какие услуги предоставляются на SAP узла PE1, передав запрос RESTCONF GET. На рисунке 9 показан пример тела отклика на запрос RESTCONF, полученного от контроллера.

```
{
  "ietf-sap-ntw:service": [
    {
      "service-type": "ietf-vpn-common:l3vpn",
      "sap": [
        {
          "sap-id": "sap#1",
          "description": "Готовы к размещению SAP",
          "attachment-interface": "GE0/6/1",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#2",
          "description": "Готовы к размещению SAP",
          "attachment-interface": "GE0/6/4",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#3",
          "description": "Описание первой точки SAP",
          "parent-termination-point": "GE0/6/4",
          "attachment-interface": "GE0/6/4.1",
          "interface-type": "ietf-sap-ntw:logical",
          "encapsulation-type": "ietf-vpn-common:vlan-type",
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          },
          "service-status": {
            "admin-status": {
              "status": "ietf-vpn-common:admin-up"
            },
            "oper-status": {
```

```
                "status": "ietf-vpn-common:op-up"
              }
            }
          }
        ]
      },
      {
        "service-type": "ietf-vpn-common:vpls",
        "sap": [
          {
            "sap-id": "sap#1",
            "description": "Готовы к размещению SAP",
            "attachment-interface": "GE0/6/1",
            "interface-type": "ietf-sap-ntw:phy",
            "role": "ietf-sap-ntw:uni",
            "allows-child-saps": true,
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            }
          },
          {
            "sap-id": "sap#2",
            "description": "Готовы к размещению SAP",
            "attachment-interface": "GE0/6/4",
            "interface-type": "ietf-sap-ntw:phy",
            "role": "ietf-sap-ntw:uni",
            "allows-child-saps": true,
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            }
          },
          {
            "sap-id": "sap#4",
            "description": "Другое описание",
            "parent-termination-point": "GE0/6/4",
            "attachment-interface": "GE0/6/4.2",
            "interface-type": "ietf-sap-ntw:logical",
            "encapsulation-type": "ietf-vpn-common:vlan-type",
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-up"
              },
              "oper-status": {
                "status": "ietf-vpn-common:op-up"
              }
            }
          }
        ]
      }
    ]
}
```

Рисунок 9. Пример тела отклика на запрос с фильтром узла.

На рисунке 10 дан пример тела отклика, полученного от контроллера сети, когда запрос включает по фильтр по типу сервиса для конкретного узла.

```
{
  "ietf-sap-ntw:service": [
    {
      "service-type": "ietf-vpn-common:l3vpn",
      "sap": [
        {
          "sap-id": "sap#1",
          "description": "Готовы к размещению SAP",
          "attachment-interface": "GE0/6/1",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
        {
          "sap-id": "sap#2",
          "description": "Готовы к размещению SAP",
          "attachment-interface": "GE0/6/4",
          "interface-type": "ietf-sap-ntw:phy",
          "role": "ietf-sap-ntw:uni",
          "allows-child-saps": true,
          "sap-status": {
            "status": "ietf-vpn-common:op-up"
          }
        },
```

```
          {
            "sap-id": "sap#3",
            "description": "Описание первой точки SAP",
            "parent-termination-point": "GE0/6/4",
            "attachment-interface": "GE0/6/4.1",
            "interface-type": "ietf-sap-ntw:logical",
            "encapsulation-type": "ietf-vpn-common:vlan-type",
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-up"
              },
              "oper-status": {
                "status": "ietf-vpn-common:op-up"
              }
            }
          }
        ]
      }
    ]
  }
```

Рисунок 10. Примера тела отклика на запрос с фильтром сервиса.

Приложение C. Пример NNI SAP - Inter-AS VPN Option A

В разделе 10 [RFC4364] рассмотрено несколько вариантов расширения услуг VPN за пределы одной автономной системы (Autonomous System или AS). Для иллюстрации здесь выбран вариант Option A, но подобные примеры можно привести и для других вариантов.

В этом варианте граничный маршрутизатор автономной системы (ASBR) напрямую соединён с ASBR соседней AS. Эти 2 ASBR связаны через несколько физических или логических интерфейсов и на каждом из ASBR имеется хотя бы 1 субинтерфейс для каждой сети VPN, которой нужно передавать свои маршруты из одной AS в другую. Оба ASBR ведут себя как узлы PE, воспринимая соседа как CE. На рисунке 11 показан упрощённый фрагмент топологии с двумя AS (A и B) с акцентом на каналы, соединяющие эти AS.

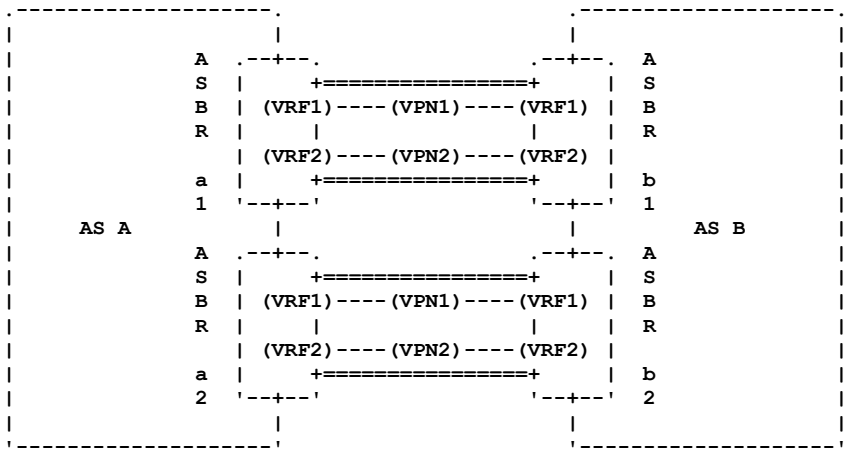

Рисунок 11. Пример Inter-AS VPN (Option A).

На рисунке 12 представлен пример тела сообщения, полученного от сетевого контроллера из AS A (с акцентом на интерфейсы NNI, показанные на рисунке 11).

```
{
  "ietf-network:networks": {
    "network": [
      {
        "network-types": {
          "ietf-sap-ntw:sap-network": {
            "service-type": [
              "ietf-vpn-common:l3vpn"
            ]
          }
        },
        "network-id": "example:an-id",
        "node": [
          {
            "node-id": "example:asbr-a1",
            "ietf-sap-ntw:service": [
              {
                "service-type": "ietf-vpn-common:l3vpn",
                "sap": [
                  {
                    "sap-id": "sap#11",
                    "description": "Родительский канал между AS link#1",
                    "role": "ietf-sap-ntw:nni",
                    "allows-child-saps": true,
                    "peer-sap-id": ["asbr-b1"],
```

```
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            }
          },
          {
            "sap-id": "sap#12",
            "description": "Родительский канал между AS link#2",
            "role": "ietf-sap-ntw:nni",
            "allows-child-saps": true,
            "peer-sap-id": ["asbr-b1"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            }
          },
          {
            "sap-id": "sap#13",
            "description": "vpn1",
            "role": "ietf-sap-ntw:nni",
            "peer-sap-id": ["asbr-b1"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-up"
              },
              "oper-status": {
                "status": "ietf-vpn-common:op-up"
              }
            }
          },
          {
            "sap-id": "sap#14",
            "description": "vpn2",
            "role": "ietf-sap-ntw:nni",
            "peer-sap-id": ["asbr-b1"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            },
            "service-status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-up"
              },
              "oper-status": {
                "status": "ietf-vpn-common:op-up"
              }
            }
          }
        ]
      }
    ]
  },
  {
    "node-id": "example:asbr-a2",
    "ietf-sap-ntw:service": [
      {
        "service-type": "ietf-vpn-common:l3vpn",
        "sap": [
          {
            "sap-id": "sap#11",
            "description": "Родительский канал между AS link#1",
            "role": "ietf-sap-ntw:nni",
            "allows-child-saps": true,
            "peer-sap-id": ["asbr-b2"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            }
          },
          {
            "sap-id": "sap#12",
            "description": "Родительский канал между AS link#2",
            "role": "ietf-sap-ntw:nni",
            "allows-child-saps": true,
            "peer-sap-id": ["asbr-b2"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            }
          },
          {
            "sap-id": "sap#21",
            "description": "vpn1",
            "role": "ietf-sap-ntw:nni",
            "peer-sap-id": ["asbr-b2"],
            "sap-status": {
              "status": "ietf-vpn-common:op-up"
            },
```

```
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  },
                  {
                    "sap-id": "sap#22",
                    "description": "vpn2",
                    "role": "ietf-sap-ntw:nni",
                    "peer-sap-id": ["asbr-b2"],
                    "sap-status": {
                      "status": "ietf-vpn-common:op-up"
                    },
                    "service-status": {
                      "admin-status": {
                        "status": "ietf-vpn-common:admin-up"
                      },
                      "oper-status": {
                        "status": "ietf-vpn-common:op-up"
                      }
                    }
                  }
                ]
              }
            ]
          }
        ]
      }
    ]
  }
}
```

Рисунок 12. Пример использования SAP для NNI.

Приложение D. Примеры применения модели SAP при создании услуг

В этом приложении приведены примеры использования модели SAP при организации услуг.

Пример топологии SAP представлен на рисунке 7 и включает 4 PE с точками SAP, а также сведения о клиентах.

Предположим, что оператор хочет организовать услугу L3VPN между двумя PE (PE3 и PE4), обслуживающими 2 CE (CE6 и CE7). Для этого оператор будет запрашивать топологию SAP и получит отклик, похожий на показанный на рисунке 7. Этот отклик показывает, что SAP с идентификаторами присоединения sap#31 и sap#43 не имеют установленных служб. Это, в частности, следует из (1) административного статуса service-status ietf-vpn-common:admin-down, для всех услуг, поддерживаемых этими двумя SAP, и (2) отсутствия аномалий, отмеченных в разделе 5. После обнаружения «свободных» SAP проверяются узлы interface-type и encapsulation-type, чтобы убедиться в совместимости запрашиваемого сервиса L3VPN с характеристиками SAP. В случае совместимости значение attachment-id можно использовать как идентификатор доступа в сеть VPN в запросе L3NM create.

Похожий процесс можно применить для организации так называемого сервиса Inter-AS VPN Option A. В отличие от предыдущего примера, предположим, что оператор хочет организовать сервис L3VPN между парой PE (PE3 и PE4), относящихся к разным AS (PE3 принадлежит AS A, а PE4 - AS B). Интерфейсы NNI между этими AS представлены на рисунке 11. Оператор AS A будет запрашивать через контроллер своей AS топологию SAP и получит не только сведения, приведённые на рисунке 7, но и показанную на рисунке 12 информацию об интерфейсах NNI. Оператор организует службу в AS A между PE3 и свободной, совместимой точкой SAP в ASBR A1. Такую же процедуру использует оператор AS B для организации службы в AS B между свободной, совместимой точкой SAP в ASBR B1 и PE4. Услуги могут предоставляться в обеих AS с использованием L3NM.

Предположим теперь, что вместо службы L3VPN оператор хочет организовать сервис L2VPN. Если interface-type является физическим портом, можно создать новую логическую точку SAP, используя модель SAP для удовлетворения потребностей службы (например, можно установить атрибут encapsulation-type ietf-vpn-common:vlan-type). После создания логической точки SAP её attachment-id применяется для организации экземпляра услуги L2NM (параграф 7.6 в [RFC9291]).

Благодарности

Спасибо Adrian Farrel, Daniel King, Dhruv Dhody, Benoit Claise, Bo Wu, Erez Segev, Raul Arco, Joe Clarke, Riyas Valiyapalathingal, Tom Petch, Olga Havel, Richard Roberts за их комментарии.

Спасибо Martin Björklund за рецензию YANG Doctors, Menachem Dodge за рецензию opsdir, Mach Chen за рецензию rtgdir, Linda Dunbar за рецензию genart и Ivaylo Petrov за рецензию secdir.

Особая благодарность Adrian Farrel за кураторскую (Shepherd) рецензию и Rob Wilton за тщательный обзор AD.

Спасибо Lars Eggert, Roman Danyliw, Zaheduzzaman Sarker за их комментарии при рецензировании в IESG.

Адреса авторов

Mohamed Boucadair (editor)
Orange
France

Email: mohamed.boucadair@orange.com

Oscar Gonzalez de Dios
Telefonica
Madrid
Spain
Email: oscar.gonzalezdedios@telefonica.com

Samier Barguil
Nokia
Madrid
Spain
Email: samier.barguil_giraldo@nokia.com

Qin Wu
Huawei
Yuhua District
101 Software Avenue
Nanjing
Jiangsu, 210012
China
Email: bill.wu@huawei.com

Victor Lopez
Nokia
Spain
Email: victor.lopez@nokia.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru