Internet Engineering Task Force (IETF)
Request for Comments: 8466
Category: Standards Track
ISSN: 2070-1721

B. Wen
Comcast
G. Fioccola, Ed.
Telecom Italia
C. Xie
China Telecom
L. Jalil
Verizon

October 2018

A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery

Модель данных YANG для предоставления услуг виртуальных сетей L2 (L2VPN)

Аннотация

В этом документе определена модель данных YANG, которая может служить для настройки конфигурации предоставляемого провайдером сервиса L2 VPN. Система управления принимает эту модель в качестве входных данных и создаёт конкретные модели конфигурации разных элементов сети для предоставления услуг. Вопросы непосредственной настройки элементов сети выходят за рамки этого документа.

Определённая в этом документе модель данных YANG включает услуги VPWS[1] («точка-точка») и VPLS[2] (многоточечные), которые используют псевдопровода с сигнализаций на основе протокола LDP[3] и BGP[4], как описано в RFC 4761 и RFC 6624.

Определённая здесь модель данных YANG соответствует архитектуре конфигурационных хранилищ NMDA[5], определённой в RFC 8342.

Статус документа

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF[6] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[7]. Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc8466.

Оглавление

[1]Virtual Private Wire Service - услуги виртуального частного провода.
[2]Virtual Private LAN Service - услуги виртуальной частной ЛВС.
[3]Label Distribution Protocol - протокол распространения меток.
[4]Border Gateway Protocol - протокол граничного шлюза.
[5]Network Management Datastore Architecture - архитектура хранилища информации сетевого управления.
[6]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[7]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

1. Введение

Этот документ определяет модель данных YANG для услуг L2 VPN (L2VPN). Модель описывает элементы конфигурации сервиса, которые могут применяться в коммуникационных протоколах между абонентами и сетевыми операторами. Эти элементы могут также служить входными данными для автоматизированных приложений управления и настройки конфигурации, которые могут генерировать конкретные конфигурации для настройки различных элементов сети, обеспечивающих сервис. Способы настройки конфигурации сетевых элементов выходят за рамки этого документа.

Дополнительное рассмотрение способов моделирования услуг с помощью YANG и связей между «абонентскими моделями сервиса», подобными описанным здесь, и конфигурационными моделями можно найти в [RFC8309] и [RFC8199]. В разделах 4 и 6 приведена более подробная информация о способах применения этой модели сервиса и её роли в общей архитектуре моделирования.

Определённая в этом документе модель YANG включает поддержку услуг VPWS (точка-точка) и VPLS (многоточечные), использующих псевдопровода с сигнализацией на основе протокола LDP и BGP, как описано в [RFC4761] и [RFC6624]. Модель соответствует архитектуре NMDA [RFC8342].

1.1. Терминология

Ниже перечислены термины, определённые в [RFC6241] и используемые здесь:

- client - клиент;
- configuration data - данные конфигурации;
- server - сервер;
- state data - данные состояния.

Ниже перечислены термины, определённые в [RFC7950] и используемые здесь:

- augment - добавление (усиление);
- data model - модель данных;
- data node - узел данных.

Терминология для описания моделей данных YANG заимствована из [RFC7950].

1.1.1. Уровни требований

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

1.2. Диаграммы деревьев

Диаграммы деревьев в этом документе используют нотацию [RFC8340].

2. Определения

Ниже приведены определения используемых в документе терминов.

Service Provider (SP) - сервис-провайдер
: Организация (обычно коммерческое предприятие), отвечающая за работу сети, которая предоставляет услуги VPN клиентам и абонентам.

Customer Edge (CE) Device - краевое устройство абонента
: Оборудование, выделенное для конкретного абонента и напрямую подключённое к одному или нескольким устройствам PE через устройства (каналы) присоединения (AC[1]). Устройства CE обычно размещаются на площадке абонента и как правило выделяются для одной сети VPN, хотя могут поддерживать и множество VPN, если для каждой применяется своё присоединение AC. Устройствами CE могут быть маршрутизаторы, мосты, коммутаторы или хосты.

Provider Edge (PE) Device - краевое устройство провайдера
: Управляемое SP оборудование, способное поддерживать множество VPN для разных абонентов и напрямую соединённое с одним или множеством устройств CE через AC. Устройства PE обычно размещаются в точке присутствия SP POP[2] и управляются SP.

Virtual Private LAN Service (VPLS) - услуги виртуальной частной ЛВС
: VPLS представляет собой услуги оператора, обеспечивающие полнофункциональную эмуляцию традиционных ЛВС. VPLS позволяет соединять несколько сегментов ЛВС через сеть пакетной коммутации (PSN[3]) в одну сеть, поведение которой похоже на единую ЛВС.

Virtual Private Wire Service (VPWS) - услуги виртуального частного провода
: VPWS представляет собой устройство «точка-точка» (т. е. канал), соединяющее два устройства CE. Канал организуется в форме логического соединения L2 через PSN. Устройства CE в сети абонента подключаются к PE в сети провайдера через AC, которые являются физическими или логическими устройствами (каналами). VPWS отличается от VPLS тем, что VPLS является многоточечным сервисом, а VPWS обеспечивает соединения «точка-точка». В некоторых реализациях набор VPWS служит для создания сети L2VPN с множеством сайтов.

[1]Attachment Circuit.
[2]Point of Presence.
[3]Packet switched network.

Pseudowire (PW) - псевдопровод

Псевдопровод представляет собой эмуляцию естественного сервиса через PSN. Эмулируемым сервисом может быть ATM, Frame Relay, Ethernet, низкоскоростной канал TDM[1] или SONET/SDH[2], а сетью PSN - MPLS, IP (IPv4 или IPv6), L2TPv3[3].

MAC-VRF

Таблица виртуальной маршрутизации и пересылки для MAC[4]-адресов в PE. Иногда используется термин VSI[5].

UNI

Интерфейс пользователя с сетью. Точка физического разделения между областями ответственности абонента и провайдера.

NNI

Интерфейс между сетями. Опорная точка, представляющая границу между двумя сетями, работающими в разных административных доменах. Сети могут относиться к одному или разным провайдерам.

Ниже перечислены используемые в документе сокращения.

BSS

Business Support System - система поддержки бизнеса.

BUM

Broadcast, Unknown Unicast, or Multicast - групповые, неизвестные индивидуальные и широковещательные (кадры).

CoS

Class of Service - класс обслуживания.

LAG

Link Aggregation Group - группы объединенных каналов.

LLDP

Link Layer Discovery Protocol - протокол обнаружения канального уровня.

OAM

Operations, Administration, and Maintenance - эксплуатация, администрирование и поддержка.

OSS

Operations Support System - система поддержки операций.

PDU

Protocol Data Unit - модуль данных протокола.

QoS

Quality of Service - качество обслуживания.

3. Модель сервиса L2 VPN

Сервис VPN уровня 2 (L2VPN[6]) представляет собой набор сайтов, уполномоченных обмениваться трафиком между собой через общую сетевую инфраструктуру на базе технологии общего назначения. Модель сервиса L2VPN (L2SM[7]), описанная в этом документе, обеспечивает базовое представление о развёртывании соответствующих услуг L2VPN через инфраструктуру общего пользования.

Этот документ представляет L2SM на основе языка моделирования данных YANG [RFC7950] в качестве формального языка, понятного человеку и пригодного для разбора программами, использующими протоколы NETCONF[8] [RFC6241] и RESTCONF [RFC8040].

Эта модель ограничена сетями VPN на основе VPWS и VPLS, как описано в [RFC4761] и [RFC6624], а также Ethernet VPN (EVPN), описанными в [RFC7432].

3.1. Типы сервиса L2 VPN

С точки зрения технологии базовые типы сервиса L2VPN включают:

- VPWS «точка-точка», использующие псевдопровода с сигнализацией LDP или L2TP [RFC6074];
- многоточечные VPLS, использующие псевдопровода с сигнализацией LDP или L2TP [RFC6074];
- многоточечные VPLS, использующие уровень управления BGP, как описано в [RFC4761] и [RFC6624];
- IPLS[9], являющиеся функциональным подмножеством услуг VPLS [RFC7436];
- EVPN на основе BGP MPLS, как описано в [RFC7432] и [RFC7209];
- EVPN VPWS, как описано в [RFC8214].

3.2. Топология физической сети L2 VPN

На рисунке 1 показана физическая топология типовой сети SP. Большинство SP использует инфраструктуру с мультисервисным ядром IP, MPLS или сегментной маршрутизации (SR[10]). Входящие кадры L2 отображаются в псевдопровод Ethernet (например, PWE3[11]) или туннель VXLAN[12] между устройствами PE. Выбор механизмов туннелирования остаётся за провайдером и не является частью L2SM.

L2VPN обеспечивает сквозные соединения L2 через инфраструктуру мультисервисного ядра между двумя или более площадками абонента. Устройства AC размещаются между CE и PE, обеспечивая доставку кадров L2 из сети абонента

[1]Time-Division Multiplexing - мультиплексирование с разделением по времени.
[2]Synchronous Optical Network / Synchronous Digital Hierarchy - синхронная оптическая сеть / синхронная цифровая иерархия.
[3]Layer 2 Tunneling Protocol version 3 - протокол туннелирования L2, версия 3.
[4]Media Access Control - управление доступом к среде.
[5]Virtual Switching Instance - экземпляр виртуальной коммутации.
[6]Layer 2 VPN.
[7]L2VPN Service Model.
[8]Network Configuration Protocol - протокол настройки конфигурации сети.
[9]IP-only LAN Service - услуги ЛВС с поддержкой только протокола IP.
[10]Segment Routing.
[11]Pseudowire Emulation Edge to Edge - сквозная эмуляция псевдопровода.
[12]Virtual Extensible Local Area Network - виртуальная расширяемая ЛВС.

через сеть доступа в провайдерскую сеть или на удалённый сайт. Граничная точка (т. е., UNI) между абонентом и SP может размещаться (1) между узлами абонента и устройством CE или (2) между устройствами CE и PE. Опорное соединение между CE и PE будет описано в L2SM.

SP может также выбрать модель «бесшовного MPLS» для создания туннеля PWE3 или VXLAN между сайтами.

SP может использовать MP-BGP[1] для автоматического обнаружения и сигнализации конечных точек туннелей PWE3 или VXLAN.

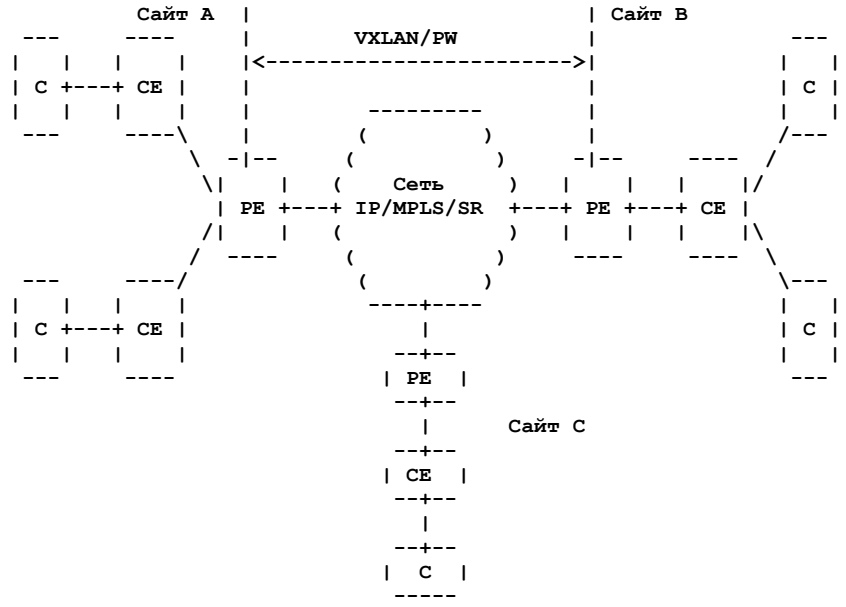

Рисунок 1. Эталонная сеть для использования L2SM.

Однако с точки зрения абонента все устройства CE будут соединены через имитируемую среду ЛВС, как показано на рисунке 2. Широковещательные и групповые пакеты передаются всем участникам одного домена мостов.

Рисунок 2. L2VPN с точки зрения абонента.

4. Использование модели данных сервиса

L2SM обеспечивает абстрактный интерфейс для запроса, настройки и управления компонентами сервиса L2VPN. Модель применяется абонентами, приобретающими соединения и другие услуги у SP, для коммуникаций с этим SP.

Типичным применением этой модели является ввод данных на уровень оркестровки, который отвечает за трансляцию этих данных в конфигурационные команды элементов сети, обеспечивающих услуги. Сетевыми элементами могут быть маршрутизаторы, а также серверы (например, AAA[2]), требуемые в сети.

Настройка конфигурации элементов сети может выполняться через командный интерфейс (CLI[3]) или иной интерфейс настройки (южную границу - southbound), такой как NETCONF [RFC6241] в комбинации с определяемой устройством и протоколом моделью YANG.

Этот способ использования модели сервиса показан на рисунке 3, а более подробное описание приведено в [RFC8309] и [RFC8199]. Разделение функций оркестровки на уровне сервиса (service orchestrator) и сети (network orchestrator) разъяснено в [RFC8309]. Применение этой модели сервиса не исчерпывается представленным примером, она может использоваться любым компонентом системы управления, но не напрямую элементами сети.

Применение и структуру этой модели следует сравнивать с сервисной моделью L3 VPN, определённой в [RFC8299].

В Metro Ethernet Forum (MEF) [MEF-6] также была разработана архитектура работы сети и сетевого управления, но работа MEF охватывает все аспекты оркестровки жизненного цикла сервиса, включая оплату (billing), соглашения об уровне обслуживания (SLA[4]), управление заказами и жизненным циклом сервиса. Работа IETF над моделью сервиса обычно более компактна и предлагает простой, самодостаточный модуль YANG. Подробности см. в [RFC8309].

5. Устройство модели данных

Структура модели L2SM позволяет провайдеру перечислить множество устройств разных типов сервиса для одного абонента. Устройство представляет сквозное соединение между двумя или более местоположениями абонента.

Модуль YANG разделен на два основных контейнера - услуги VPN (vpn-services) и сайты (sites). Контейнер vpn-svc в иерархии vpn-services определяет глобальные параметры сервиса VPN для конкретного абонента.

Сайт имеет по меньше мере одно подключение к сети (т. е. доступ сайта в сеть обеспечивающий связь и другими сайтами, как указано в параграфе 5.3.2) и может иметь множество подключений в многодомном случае. Подключение сайта к сети выполняется через опорное соединение (носитель - bearer) на канальном уровне (L2). «Носитель»

[1]Multiprotocol BGP - многопротокольный BGP.
[2]Authentication, Authorization, and Accounting - проверка подлинности, проверка полномочий, учет.
[3]Command Line Interface - интефейс командной строки.
[4]Service Level Agreement.

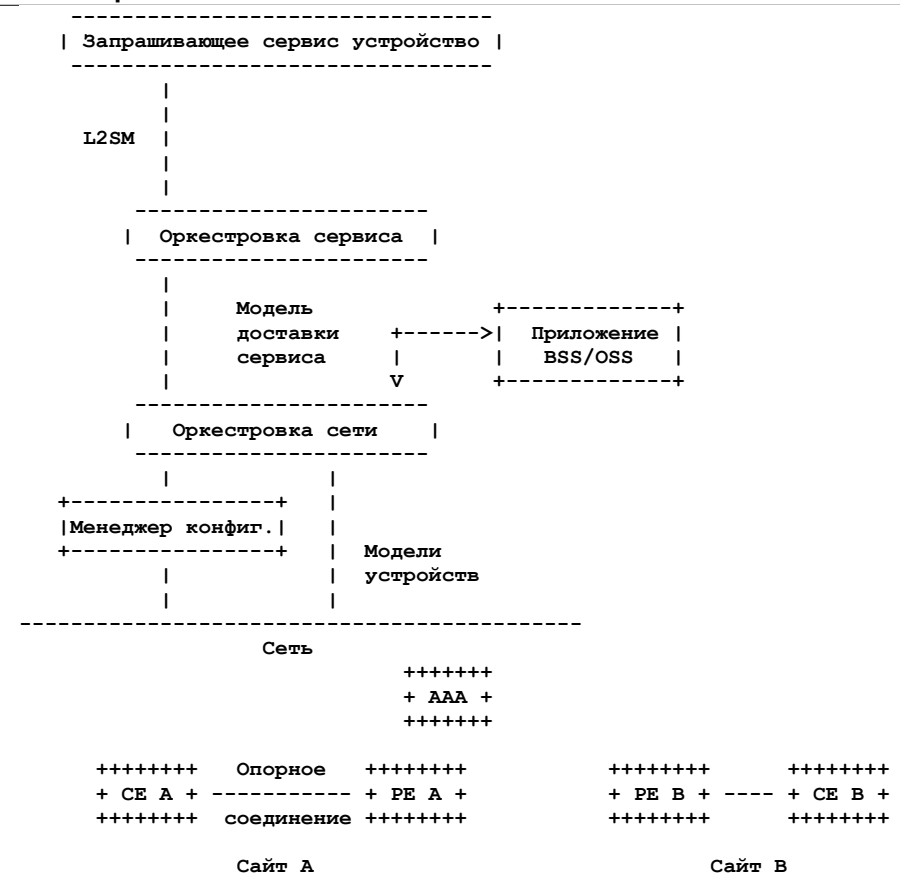

Рисунок 3. Эталонная архитектура для использования L2SM.

относится к свойствам ниже уровня L2, а «соединение» к протокольным свойствам L2. Соединение-носитель может динамически выделяться SP, а абонент может задавать некоторые ограничения для управления местом соединения.

Полномочия на обмен трафиком предоставляются на основе политики или топологии VPN, которая определяет правила обмена маршрутной информацией между сайтами.

Сквозные многосегментные соединения могут быть реализованы на основе комбинации связности на уровне сайтов и сегментов.

На рисунке 4 показана общая структура модуля YANG.

```
module: ietf-l2vpn-svc
+--rw l2vpn-svc
  +--rw vpn-profiles
  |  +--rw valid-provider-identifiers
  |     +--rw cloud-identifier*  string{cloud-access}?
  |     +--rw qos-profile-identifier* string
  |     +--rw bfd-profile-identifier* string
  |     +--rw remote-carrier-identifier* string
  +--rw vpn-services
  |  +--rw vpn-service* [vpn-id]
  |     +--rw vpn-id                      svc-id
  |     +--rw vpn-svc-type?               identityref
  |     +--rw customer-name?              string
  |     +--rw svc-topo?                   identityref
  |     +--rw cloud-accesses {cloud-access}?
  |     |  +--rw cloud-access* [cloud-identifier]
  |     |     +--rw cloud-identifier
  |     |     |    -> /l2vpn-svc/vpn-profiles/
  |     |     |      valid-provider-identifiers/cloud-identifier
  |     |     +--rw (list-flavor)?
  |     |        +--:(permit-any)
  |     |        |  +--rw permit-any?         empty
  |     |        +--:(deny-any-except)
  |     |        |  +--rw permit-site*
  |     |        |  :    -> /l2vpn-svc/sites/site/site-id
  |     |        +--:(permit-any-except)
  |     |           +--rw deny-site*
  |     |                -> /l2vpn-svc/sites/site/site-id
  |     +--rw frame-delivery {frame-delivery}?
  |     |  +--rw customer-tree-flavors
  |     |  |  +--rw tree-flavor*   identityref
  |     |  +--rw bum-frame-delivery
  |     |  |  +--rw bum-frame-delivery* [frame-type]
  |     |  |     +--rw frame-type       identityref
  |     |  |     +--rw delivery-mode?   identityref
  |     |  +--rw multicast-gp-port-mapping    identityref
  |     +--rw extranet-vpns {extranet-vpn}?
```

```
|     |  +--rw extranet-vpn* [vpn-id]
|     |     +--rw vpn-id              svc-id
|     |     +--rw local-sites-role?   identityref
|     +--rw ce-vlan-preservation        boolean
|     +--rw ce-vlan-cos-preservation    boolean
|     +--rw carrierscarrier?            boolean {carrierscarrier}?
+--rw sites
  +--rw site* [site-id]
   +--rw site-id                                string
   +--rw site-vpn-flavor?                       identityref
   +--rw devices
   |  +--rw device* [device-id]
   |     +--rw device-id     string
   |     +--rw location
   |     |    -> ../../../locations/location/location-id
   |     +--rw management
   |        +--rw transport?   identityref
   |        +--rw address?     inet:ip-address
   +--rw management
   |  +--rw type    identityref
   +--rw locations
   |  +--rw location* [location-id]
   |     +--rw location-id     string
   |     +--rw address?        string
   |     +--rw postal-code?    string
   |     +--rw state?          string
   |     +--rw city?           string
   |     +--rw country-code?   string
   +--rw site-diversity {site-diversity}?
   |  +--rw groups
   |     +--rw group* [group-id]
   |        +--rw group-id    string
   +--rw vpn-policies
   |  +--rw vpn-policy* [vpn-policy-id]
   |     +--rw vpn-policy-id    string
   |     +--rw entries* [id]
   |        +--rw id         string
   |        +--rw filters
   |        |  +--rw filter* [type]
   |        |     +--rw type       identityref
   |        |     +--rw lan-tag*   uint32 {lan-tag}?
   |        +--rw vpn* [vpn-id]
   |           +--rw vpn-id
   |           |    -> /l2vpn-svc/vpn-services/
   |           |            vpn-service/vpn-id
   |           +--rw site-role?   identityref
   +--rw service
   |  +--rw qos {qos}?
   |  |  +--rw qos-classification-policy
   |  |  |  +--rw rule* [id]
   |  |  |     +--rw id                    string
   |  |  |     +--rw (match-type)?
   |  |  |     |  +--:(match-flow)
   |  |  |     |  |  +--rw match-flow
   |  |  |     |  |     +--rw dscp?           inet:dscp
   |  |  |     |  |     +--rw dot1q?          uint16
   |  |  |     |  |     +--rw pcp?            uint8
   |  |  |     |  |     +--rw src-mac?        yang:mac-address
   |  |  |     |  |     +--rw dst-mac?        yang:mac-address
   |  |  |     |  |     +--rw color-type?     identityref
   |  |  |     |  |     +--rw target-sites*
   |  |  |     |  |     |               svc-id {target-sites}?
   |  |  |     |  |     +--rw any?            empty
   |  |  |     |  |     +--rw vpn-id?         svc-id
   |  |  |     |  +--:(match-application)
   |  |  |     |     +--rw match-application?   identityref
   |  |  |     +--rw target-class-id?     string
   |  |  +--rw qos-profile
   |  |     +--rw (qos-profile)?
   |  |        +--:(standard)
   |  |        |  +--rw profile?
   |  |        |       -> /l2vpn-svc/vpn-profiles/
   |  |        |              valid-provider-identifiers/
   |  |        |              qos-profile-identifier
   |  |        +--:(custom)
   |  |           +--rw classes {qos-custom}?
   |  |              +--rw class* [class-id]
   |  |                 +--rw class-id        string
   |  |                 +--rw direction?      identityref
   |  |                 +--rw policing?       identityref
   |  |                 +--rw byte-offset?    uint16
   |  |                 +--rw frame-delay
   |  |                 |  +--rw (flavor)?
   |  |                 |     +--:(lowest)
   |  |                 |     |  +--rw use-lowest-latency? empty
   |  |                 |     +--:(boundary)
```

```
|  |                 |        +--rw delay-bound?     uint16
|  |                 +--rw frame-jitter
|  |                 |  +--rw (flavor)?
|  |                 |     +--:(lowest)
|  |                 |     |  +--rw use-lowest-jitter? empty
|  |                 |     +--:(boundary)
|  |                 |        +--rw delay-bound?     uint32
|  |                 +--rw frame-loss
|  |                 |  +--rw rate?   decimal64
|  |                 +--rw bandwidth
|  |                    +--rw guaranteed-bw-percent decimal64
|  |                    +--rw end-to-end?           empty
|  +--rw carrierscarrier {carrierscarrier}?
|     +--rw signaling-type?   identityref
+--rw broadcast-unknown-unicast-multicast {bum}?
|  +--rw multicast-site-type?            enumeration
|  +--rw multicast-gp-address-mapping* [id]
|  |  +--rw id                 uint16
|  |  +--rw vlan-id            uint16
|  |  +--rw mac-gp-address     yang:mac-address
|  |  +--rw port-lag-number?   uint32
|  +--rw bum-overall-rate?     uint32
|  +--rw bum-rate-per-type* [type]
|     +--rw type    identityref
|     +--rw rate?   uint32
+--rw mac-loop-prevention {mac-loop-prevention}?
|  +--rw protection-type?   identityref
|  +--rw frequency?         uint32
|  +--rw retry-timer?       uint32
+--rw access-control-list
|  +--rw mac* [mac-address]
|     +--rw mac-address    yang:mac-address
+--ro actual-site-start?   yang:date-and-time
+--ro actual-site-stop?    yang:date-and-time
+--rw bundling-type?       identityref
+--rw default-ce-vlan-id   uint32
+--rw site-network-accesses
   +--rw site-network-access* [network-access-id]
   +--rw network-access-id                string
   +--rw remote-carrier-name?             string
   +--rw type?                            identityref
   +--rw (location-flavor)
   |  +--:(location)
   |  |  +--rw location-reference?
   |  |       -> ../../../locations/location/
   |  |               location-id
   |  +--:(device)
   |     +--rw device-reference?
   |          -> ../../../devices/device/device-id
   +--rw access-diversity {site-diversity}?
   |  +--rw groups
   |  |  +--rw group* [group-id]
   |  |     +--rw group-id    string
   |  +--rw constraints
   |     +--rw constraint* [constraint-type]
   |        +--rw constraint-type    identityref
   |        +--rw target
   |           +--rw (target-flavor)?
   |              +--:(id)
   |              |  +--rw group* [group-id]
   |              |     +--rw group-id    string
   |              +--:(all-accesses)
   |              |  +--rw all-other-accesses?   empty
   |              +--:(all-groups)
   |                 +--rw all-other-groups?     empty
   +--rw bearer
   |  +--rw requested-type {requested-type}?
   |  |  +--rw type?     string
   |  |  +--rw strict?   boolean
   |  +--rw always-on?         boolean {always-on}?
   |  +--rw bearer-reference?  string {bearer-reference}?
   +--rw connection
   |  +--rw encapsulation-type?    identityref
   |  +--rw eth-inf-type?          identityref
   |  +--rw tagged-interface
   |  |  +--rw type?               identityref
   |  |  +--rw dot1q-vlan-tagged {dot1q}?
   |  |  |  +--rw tg-type?    identityref
   |  |  |  +--rw cvlan-id    uint16
   |  |  +--rw priority-tagged
   |  |  |  +--rw tag-type?   identityref
   |  |  +--rw qinq {qinq}?
   |  |  |  +--rw tag-type?   identityref
   |  |  |  +--rw svlan-id    uint16
   |  |  |  +--rw cvlan-id    uint16
   |  |  +--rw qinany {qinany}?
```

```
|  |  |  +--rw tag-type?   identityref
|  |  |  +--rw svlan-id    uint16
|  |  +--rw vxlan {vxlan}?
|  |     +--rw vni-id       uint32
|  |     +--rw peer-mode?   identityref
|  |     +--rw peer-list* [peer-ip]
|  |        +--rw peer-ip    inet:ip-address
|  +--rw untagged-interface
|  |  +--rw speed?                 uint32
|  |  +--rw mode?                  neg-mode
|  |  +--rw phy-mtu?               uint32
|  |  +--rw lldp?                  boolean
|  |  +--rw oam-802.3ah-link {oam-3ah}?
|  |  |  +--rw enabled?   boolean
|  |  +--rw uni-loop-prevention?   boolean
|  +--rw lag-interfaces {lag-interface}?
|  |  +--rw lag-interface* [index]
|  |     +--rw index    string
|  |     +--rw lacp {lacp}?
|  |        +--rw enabled?           boolean
|  |        +--rw mode?              neg-mode
|  |        +--rw speed?             uint32
|  |        +--rw mini-link-num?     uint32
|  |        +--rw system-priority?   uint16
|  |        +--rw micro-bfd {micro-bfd}?
|  |        |  +--rw enabled?      enumeration
|  |        |  +--rw interval?     uint32
|  |        |  +--rw hold-timer?   uint32
|  |        +--rw bfd {bfd}?
|  |        |  +--rw enabled?      boolean
|  |        |  +--rw (holdtime)?
|  |        |     +--:(profile)
|  |        |     |  +--rw profile-name?
|  |        |     |    -> /l2vpn-svc/
|  |        |     |         vpn-profiles/
|  |        |     |       valid-provider-identifiers/
|  |        |     |      bfd-profile-identifier
|  |        |     +--:(fixed)
|  |        |        +--rw fixed-value?    uint32
|  |        +--rw member-links
|  |        |  +--rw member-link* [name]
|  |        |     +--rw name                string
|  |        |     +--rw speed?              uint32
|  |        |     +--rw mode?               neg-mode
|  |        |     +--rw link-mtu?           uint32
|  |        |     +--rw oam-802.3ah-link {oam-3ah}?
|  |        |        +--rw enabled?  boolean
|  |        +--rw flow-control?      boolean
|  |        +--rw lldp?              boolean
|  +--rw cvlan-id-to-svc-map* [svc-id]
|  |  +--rw svc-id
|  |  |    -> /l2vpn-svc/vpn-services/vpn-service/
|  |  |          vpn-id
|  |  +--rw cvlan-id* [vid]
|  |     +--rw vid    uint16
|  +--rw l2cp-control {l2cp-control}?
|  |  +--rw stp-rstp-mstp?    control-mode
|  |  +--rw pause?            control-mode
|  |  +--rw lacp-lamp?        control-mode
|  |  +--rw link-oam?         control-mode
|  |  +--rw esmc?             control-mode
|  |  +--rw l2cp-802.1x?      control-mode
|  |  +--rw e-lmi?            control-mode
|  |  +--rw lldp?             boolean
|  |  +--rw ptp-peer-delay?   control-mode
|  |  +--rw garp-mrp?         control-mode
|  +--rw oam {oam}
|     +--rw md-name         string
|     +--rw md-level        uint16
|     +--rw cfm-802.1-ag* [maid]
|     |  +--rw maid                      string
|     |  +--rw mep-id?                   uint32
|     |  +--rw mep-level?                uint32
|     |  +--rw mep-up-down?              enumeration
|     |  +--rw remote-mep-id?            uint32
|     |  +--rw cos-for-cfm-pdus?         uint32
|     |  +--rw ccm-interval?             uint32
|     |  +--rw ccm-holdtime?             uint32
|     |  +--rw alarm-priority-defect?    identityref
|     |  +--rw ccm-p-bits-pri?       ccm-priority-type
|     +--rw y-1731* [maid]
|        +--rw maid                            string
|        +--rw mep-id?                         uint32
|        +--rw type?                        identityref
|        +--rw remote-mep-id?                  uint32
|        +--rw message-period?                 uint32
```

```
|        +--rw measurement-interval?          uint32
|        +--rw cos?                           uint32
|        +--rw loss-measurement?              boolean
|        +--rw synthetic-loss-measurement?    boolean
|        +--rw delay-measurement
|        |  +--rw enable-dm?   boolean
|        |  +--rw two-way?     boolean
|        +--rw frame-size?                    uint32
|        +--rw session-type?                enumeration
+--rw availability
|  +--rw access-priority?   uint32
|  +--rw (redundancy-mode)?
|     +--:(single-active)
|     |  +--rw single-active?     empty
|     +--:(all-active)
|        +--rw all-active?        empty
+--rw vpn-attachment
|  +--rw (attachment-flavor)
|     +--:(vpn-id)
|     |  +--rw vpn-id?
|     |  |    -> /l2vpn-svc/vpn-services/
|     |  |            vpn-service/vpn-id
|     |  +--rw site-role?              identityref
|     +--:(vpn-policy-id)
|        +--rw vpn-policy-id?
|             -> ../../../../vpn-policies/
|                     vpn-policy/vpn-policy-id
+--rw service
|  +--rw svc-bandwidth {input-bw}?
|  |  +--rw bandwidth* [direction type]
|  |     +--rw direction    identityref
|  |     +--rw type         identityref
|  |     +--rw cos-id?      uint8
|  |     +--rw vpn-id?      svc-id
|  |     +--rw cir          uint64
|  |     +--rw cbs          uint64
|  |     +--rw eir?         uint64
|  |     +--rw ebs?         uint64
|  |     +--rw pir?         uint64
|  |     +--rw pbs?         uint64
|  +--rw svc-mtu            uint16
|  +--rw qos {qos}?
|  |  +--rw qos-classification-policy
|  |  |  +--rw rule* [id]
|  |  |     +--rw id                    string
|  |  |     +--rw (match-type)?
|  |  |     |  +--:(match-flow)
|  |  |     |  |  +--rw match-flow
|  |  |     |  |     +--rw dscp?           inet:dscp
|  |  |     |  |     +--rw dot1q?          uint16
|  |  |     |  |     +--rw pcp?            uint8
|  |  |     |  |     +--rw src-mac?  yang:mac-address
|  |  |     |  |     +--rw dst-mac?  yang:mac-address
|  |  |     |  |     +--rw color-type?     identityref
|  |  |     |  |     +--rw target-sites*
|  |  |     |  |     |          svc-id {target-sites}?
|  |  |     |  |     +--rw any?            empty
|  |  |     |  |     +--rw vpn-id?         svc-id
|  |  |     |  +--:(match-application)
|  |  |     |     +--rw match-application? identityref
|  |  |     +--rw target-class-id?     string
|  |  +--rw qos-profile
|  |     +--rw (qos-profile)?
|  |        +--:(standard)
|  |        |  +--rw profile?
|  |        |       -> /l2vpn-svc/vpn-profiles/
|  |        |             valid-provider-identifiers/
|  |        |             qos-profile-identifier
|  |        +--:(custom)
|  |           +--rw classes {qos-custom}?
|  |              +--rw class* [class-id]
|  |                 +--rw class-id        string
|  |                 +--rw direction?      identityref
|  |                 +--rw policing?       identityref
|  |                 +--rw byte-offset?    uint16
|  |                 +--rw frame-delay
|  |                 |  +--rw (flavor)?
|  |                 |     +--:(lowest)
|  |                 |     |  +--rw use-lowest-latency?
|  |                 |     |                     empty
|  |                 |     +--:(boundary)
|  |                 |        +--rw delay-bound? uint16
|  |                 +--rw frame-jitter
|  |                 |  +--rw (flavor)?
|  |                 |     +--:(lowest)
|  |                 |     |  +--rw use-lowest-jitter?
```

```
|  |                 |     |                      empty
|  |                 |     +--:(boundary)
|  |                 |        +--rw delay-bound? uint32
|  |                 +--rw frame-loss
|  |                 |  +--rw rate?   decimal64
|  |                 +--rw bandwidth
|  |                    +--rw guaranteed-bw-percent
|  |                    |                   decimal64
|  |                    +--rw end-to-end?       empty
|  +--rw carrierscarrier {carrierscarrier}?
|     +--rw signaling-type?   identityref
+--rw broadcast-unknown-unicast-multicast {bum}?
|  +--rw multicast-site-type?           enumeration
|  +--rw multicast-gp-address-mapping* [id]
|  |  +--rw id                  uint16
|  |  +--rw vlan-id             uint16
|  |  +--rw mac-gp-address      yang:mac-address
|  |  +--rw port-lag-number?    uint32
|  +--rw bum-overall-rate?              uint32
|  +--rw bum-rate-per-type* [type]
|     +--rw type    identityref
|     +--rw rate?   uint32
+--rw mac-loop-prevention {mac-loop-prevention}?
|  +--rw protection-type?   identityref
|  +--rw frequency?         uint32
|  +--rw retry-timer?       uint32
+--rw access-control-list
|  +--rw mac* [mac-address]
|     +--rw mac-address    yang:mac-address
+--rw mac-addr-limit
+--rw limit-number?    uint16
+--rw time-interval?   uint32
+--rw action?          identityref
```

Рисунок 4. Общая структура модуля YANG.

5.1. Свойства и их дополнение

Определённая в этом документе модель включает множество функций, которые обеспечивают возможность модульной реализации. Например, параметры L2 (параграф 5.3.2.2), предлагаемые абоненту, могут включаться и выключаться с помощью функций (возможностей). Модель также определяет некоторые возможности для расширенных опций, таких как поддержка Extranet VPN (параграф 5.2.4), разнородность сайтов (параграф 5.3) и QoS (параграф 5.10.2).

Как и многие другие модели YANG, данная модель может быть дополнена для реализации новых вариантов поведения или специальных возможностей. Например, эта модель определяет VXLAN [RFC7348] для инкапсуляции пакетов Ethernet и если инкапсуляция VXLAN не совсем удовлетворяет требования сервиса, можно реализовать новые опции путём дополнения.

5.2. Обзор сервиса VPN

Элемент списка vpn-service содержит базовую информацию о сервисе VPN. Элемент vpn-id в списке vpn-service задаёт внутреннюю ссылку для данного сервиса VPN. Этот идентификатор является внутренним для организации, отвечающей за поддержку сервиса VPN.

Список vpn-service содержит перечисленные ниже характеристики.

Информация абонента (customer-name)
Служит для идентификации абонента (заказчика).

Тип сервиса VPN (vpn-svc-type)
Служит для указания типа сервиса VPN. Идентификатор допускает произвольное кодирование для локального администрирования услуг VPN. Отметим, что для расширения базового идентификатора может применяться дополнительный.

Доступ в облако (cloud-access)
Всем сайтам в L2VPN **следует** по умолчанию предоставлять доступ в облако. Контейнер cloud-access содержит правила предоставления полномочий. Для идентификации целевого сервиса служит указатель облака. Идентификатор является локальным для каждого домена администрирования.

Топология сервиса (svc-topo)
Служит для указания требуемой топологии сервиса VPN.

Служба доставки кадров (frame-delivery)
Определяет поддержку доставки кадров, требуемую для L2VPN, например, групповая, индивидуальная или широковещательная доставка.

Extranet VPN (extranet-vpns)
Указывает, что для конкретной VPN требуется доступ к ресурсам, находящимся в других VPN.

5.2.1. Тип сервиса VPN

Параметр vpn-svc-type определяет тип сервиса для предоставляемых провайдером услуг L2VPN. Текущая версия модели поддерживает шесть вариантов:

- VPWS «точка-точка» для соединения двух сайтов абонента;
- VPWS «точка-точка» или «точка-многоточка» для соединения множества сайтов абонента [RFC8214];
- многоточечные VPLS для соединения множества сайтов абонента;

- многоточечные VPLS для соединения одного или множества корневых сайтов с набором отделений (leaf site), но без связи между этими отделениями;
- EVPN [RFC7432] для соединения множества сайтов абонента;
- EVPN VPWS между двумя или множеством сайтов абонента, как указано в [RFC8214].

Другие типы сервиса L2VPN могут включаться через дополнения. Отметим, что сервис EPL[1] или EVPL[2] относится к типу E-Line[3] [MEF-6] или EVC[4], а сервис EP-LAN[5] или EVP-LAN[6] - к типу E-LAN[7] [MEF-6] или многоточечному EVC.

5.2.2. Топология сервиса VPN

Рассматриваемые здесь типы топологии сервиса VPN могут при необходимости использоваться для настройки конфигурации. Описанный в документе модуль поддерживает полносвязные соединения (any-to-any), звезду (Hub-and-Spoke, где концентраторы могут обмениваться трафиком) и Hub-and-Spoke Disjoint (концентраторы не могут обмениваться трафиком). Новые варианты топологии могут быть реализованы в дополнениях. По умолчанию применяется топология any-to-any.

5.2.2.1. Выделение RT

Основанные на PE услуги L2 VPN (такие как VPLS и EVPN с применением BGP в качестве сигнального протокола) могут строиться с использованием целей маршрутов (RT[8]), как описано в [RFC4364] и [RFC7432]. Предполагается, что система управления автоматически выделяет набор RT при получении запроса на организацию сервиса VPN. Способ выделения RT системой управления выходит за рамки документа, но можно предусмотреть несколько вариантов, как описано в параграфе 6.2.1.1 [RFC8299].

5.2.2.2. Каждый с каждым (Any-to-Any)

Рисунок 5. Топология сервиса Any-to-Any VPN.

В топологии сервиса VPN «any-to-any » все сайты VPN могут взаимодействовать между собой без ограничений. В этой модели предполагается, что система управления, получающая запрос на организацию сервиса any-to-any L2VPN, назначит, а затем настроит MAC-VRF и RT на соответствующих устройствах PE. Для полносвязной топологии в общем случае требуется одно значение RT и каждая таблица MAC-VRF импортирует и экспортирует это значение RT.

5.2.2.3. Концентратор и лучи (Hub-and-Spoke)

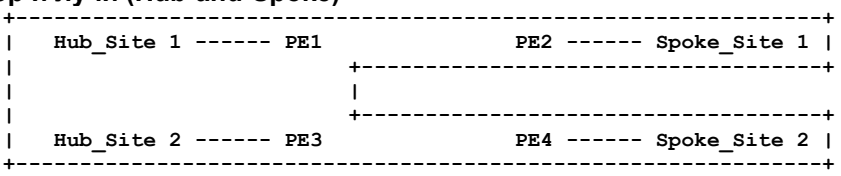

Рисунок 6. Топология сервиса Hub-and-Spoke VPN.

В топологии сервиса VPN Hub-and-Spoke

- все сайты-лучи (Spoke) могут взаимодействовать только с сайтами-концентраторами (Hub), т. е. лучи не могут взаимодействовать между собой;
- концентраторы могут взаимодействовать между собой.

В этой модели предполагается, что система управления, получившая запрос на организацию сервиса Hub-and-Spoke L2VPN, назначит, а затем настроит MAC-VRF и RT на соответствующих устройствах PE. Для Hub-and-Spoke обычно нужны два значения RT (одно для Hub-маршрутов, другое для Spoke). Таблица Hub MAC-VRF, подключающая Hub-сайты, будет экспортировать Hub-маршруты с Hub RT и импортировать Spoke-маршруты через Spoke RT. Будут также импортироваться Hub RT для поддержки коммуникаций между Hub-сайтами. Таблица Spoke MAC-VRF, подключающая Spoke-сайты, будет экспортировать Spoke-маршруты со Spoke RT и импортировать Hub-маршруты через Hub RT.

5.2.2.4. Hub-and-Spoke Disjoint

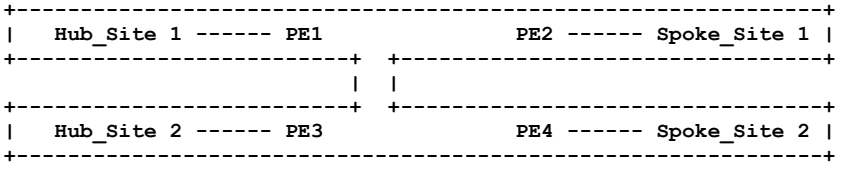

Рисунок 7. Топология сервиса Hub-and-Spoke-Disjoint VPN.

В топологии сервиса VPN Hub-and-Spoke-Disjoint

[1]Ethernet Private Line - частная линия Ethernet.
[2]Ethernet Virtual Private Line - виртуальная частная линия Ethernet.
[3]Ethernet Line - линия Ethernet.
[4]Ethernet Virtual Circuit - виртуальной устройство (канал) Ethernet.
[5]Ethernet Private LAN - частная ЛВС Ethernet.
[6]Ethernet Virtual Private LAN - виртуальная частная ЛВС Ethernet.
[7]Ethernet LAN - ЛВС Ethernet.
[8]Route Target.

- все сайты-лучи (Spoke) могут взаимодействовать только с сайтами-концентраторами (Hub), т. е. лучи не могут взаимодействовать между собой;
- концентраторы не могут взаимодействовать между собой.

В этой модели предполагается, что система управления, получившая запрос на организацию сервиса Hub-and-Spoke-Disjoint L2VPN назначит, а затем настроит VRF и RT для соответствующих устройств PE. В случае Hub-and-Spoke-Disjoint требуется по меньшей мере два значения RT (хотя бы одно для Hub-маршрутов и хотя бы одно для Spoke). Таблица Hub VRF, подключающая сайты Hub, будет экспортировать Hub-маршруты с RT и импортировать Spoke-маршруты через Spoke RT. Таблица Spoke VRF, подключающая сайты Spoke, будет экспортировать Spoke-маршруты со Spoke RT и импортировать Hub-маршруты через Hub RT.

Система управления **должна** учитывать ограничения для соединений Hub-and-Spoke как в предыдущем случае.

Топологию Hub-and-Spoke Disjoint можно рассматривать как множество Hub-and-Spoke VPN (одна сеть на Hub), использующих общий набор сайтов Spoke.

5.2.3. Доступ к облаку

Эта модель предполагает настройку доступа к облаку через контейнер cloud-access. Использование контейнера cloud-access нацелено на доступ к облачным службам общего пользования и в Internet. Контейнер cloud-access обеспечивает параметры правил предоставления полномочий. Отметим, что в этой модели предполагается некая общность доступа к облакам общего пользования и сети Internet, поэтому такие варианты доступа не различаются. При необходимости для доступа в Internet можно добавить отдельную метку путём дополнения.

Доступ к частным облакам можно организовать через контейнер site, как описано в параграфе 5.3, с использованием совместимого с сайтом типа интерфейса NNI.

Идентификатор облака служит для указания целевого сервиса. Этот идентификатор является локальным для административного домена.

По умолчанию всем сайтам в L2VPN **следует** разрешать доступ в облако или Internet. Если требуются ограничения, пользователь **может** настроить некоторые ограничения для отдельных сайтов или узлов с помощью правил, т. е. листа-списка permit-site или deny-site. Лист-список permit-site определяет список сайтов, имеющих полномочия для доступа к облаку, deny-site определяет сайты, которым доступ запрещён. Модель поддерживает варианты deny-any-except (запрет всем кроме …) и permit-any-except (разрешить всем кроме ...).

Настройка ограничений в сетевых элементах выходит за рамки документа.

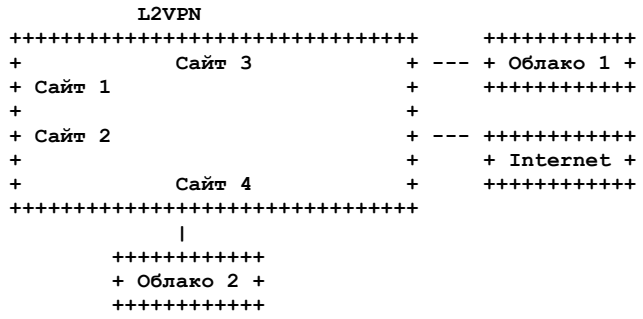

Рисунок 8. Пример конфигурации доступа в облако.

На рисунке 8 показан пример VPN с глобальным доступом в Internet путём создания контейнера cloud-access, указывающего идентификатор контейнера для доступа в Internet (см. приведённый ниже код XML [W3C.REC-xml-20081126]). Уполномоченных сайтов не задано, поскольку доступ в Internet нужен для всех сайтов.

```
<?xml version="1.0"?>
   <l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
   <vpn-services>
   <vpn-service>
   <vpn-id>123456487</vpn-id>
  <cloud-accesses>
   <cloud-access>
      <cloud-identifier>INTERNET</cloud-identifier>
   </cloud-access>
  </cloud-accesses>
  <ce-vlan-preservation>true</ce-vlan-preservation>
  <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
  </vpn-service>
  </vpn-services>
</l2vpn-svc>
```

Если Сайтам 1 и 2 нужно доступ в Облако 1, создаётся новый контейнер cloud-access с идентификатором Облака 1. Лист-список permit-site в нем указывает Сайты 1 и 2.

```
<?xml version="1.0"?>
   <l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
    <vpn-services>
     <vpn-service>
     <vpn-id>123456487</vpn-id>
     <cloud-accesses>
      <cloud-access>
        <cloud-identifier>Cloud1</cloud-identifier>
        <permit-site>site1</permit-site>
        <permit-site>site2</permit-site>
```

```
        </cloud-access>
       </cloud-accesses>
      <ce-vlan-preservation>true</ce-vlan-preservation>
      <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
     </vpn-service>
     </vpn-services>
  </l2vpn-svc>
```

Если всем сайтам кроме Сайта 1 нужен доступ в Облако 2, создаётся контейнер cloud-access с идентификатором Облака 2, в котором лист-список deny-site указывает Сайт 1.

```
<?xml version="1.0"?>
  <l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
    <vpn-services>
     <vpn-service>
       <vpn-id>123456487</vpn-id>
      <cloud-accesses>
       <cloud-access>
        <cloud-identifier>Cloud2</cloud-identifier>
        <deny-site>site1</deny-site>
       </cloud-access>
      </cloud-accesses>
     <ce-vlan-preservation>true</ce-vlan-preservation>
     <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
    </vpn-service>
  </vpn-services>
</l2vpn-svc>
```

5.2.4. Сети Extranet VPN

В некоторых случаях отдельным VPN нужен доступ к внешним ресурсам (серверы, хосты и т. п.). Эти ресурсы могут размещаться в другой сети VPN.

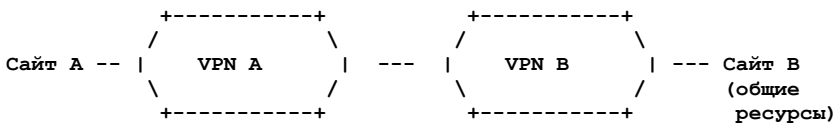

Рисунок 9. Пример общего ресурса VPN.

Как показано на рисунке 9, VPN B имеет на Сайте B отдельные ресурсы, которые должны быть доступны некоторым абонентам/партнёрам. В частности, для VPN A должен обеспечиваться доступ к этим ресурсам VPN B.

Такие варианты связи между VPN могут быть реализованы на основе политики VPN, как описано в параграфе 5.5.2.2. Однако в некоторых простых случаях отдельной сети VPN (VPN A) нужен доступ ко всем ресурсам другой VPN (VPN B). Модель обеспечивает простой способ такого соединения за счёт использования контейнера extranet-vpns.

Контейнер extranet-vpns определяет список VPN, к которым заданная сеть VPN хочет получить доступ. Контейнеры extranet-vpns используются в абонентских VPN, требующих доступа к ресурсам других VPN. На рисунке 9 для предоставления VPN A доступа в VPN B нужно настроить контейнер extranet-vpns для VPN A с записью, соответствующей VPN B. Настроек сервиса для VPN B не требуется.

Следует отметить, что не требуется настраивать конфигурацию VPN B, если в VPN A эта VPN B указана как внешняя сеть (extranet). Все сайты VPN B будут доступны всем сайтам VPN A.

Лист site-role указывает роль локальных сайтов VPN в топологии сервиса extranet VPN. Определения ролей приведены в параграфе 5.4.

В приведённом ниже примере VPN A обращается к ресурсам VPN B через соединение extranet. Для сайтов VPN A нужна роль Spoke, поскольку этим сайтам не разрешается взаимодействовать между собой через соединение extranet.

```
<?xml version="1.0"?>
  <l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
   <vpn-services>
     <vpn-service>
       <vpn-id>VPNB</vpn-id>
         <svc-topo>hub-spoke</svc-topo>
        <ce-vlan-preservation>true</ce-vlan-preservation>
        <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
     </vpn-service>
     <vpn-service>
        <vpn-id>VPNA</vpn-id>
          <svc-topo>any-to-any</svc-topo>
             <extranet-vpns>
               <extranet-vpn>
                <vpn-id>VPNB</vpn-id>
                <local-sites-role>spoke-role</local-sites-role>
               </extranet-vpn>
             </extranet-vpns>
        <ce-vlan-preservation>true</ce-vlan-preservation>
        <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
    </vpn-service>
   </vpn-services>
 </l2vpn-svc>
```

Эта модель не определяет способов создания конфигурации extranet в сети.

В любом более сложном варианте соединений между VPN (например, доступ лишь некоторых сайтов VPN A только к некоторой части сайтов VPN B) требуется присоединение VPN, описанное в параграфе 5.5.2, и, в частности, политика VPN, описанная в параграфе 5.5.2.2.

5.2.5. Услуги доставки кадров

Если для L2VPN поддерживается доставка индивидуальных кадров с неизвестными адресами, а также групповых и широковещательных кадров (BUM), при запросе сервиса потребуется указать некоторые глобальные параметры доставки кадров. Когда CE передаёт пакеты BUM, на входном PE выполняется репликация и необходимо поддерживать три типа кадров.

Пользователи этой модели должны обеспечить варианты деревьев, которые будут применяться абонентами в L2VPN (customer-tree-flavors). Определённая в документе модель поддерживает двунаправленные (bidirectional), совместно используемые (shared) и основанные на источнике (source-based) деревья, а с помощью дополнений могут поддерживаться другие типы. Одновременно может использоваться множество типов деревьев.

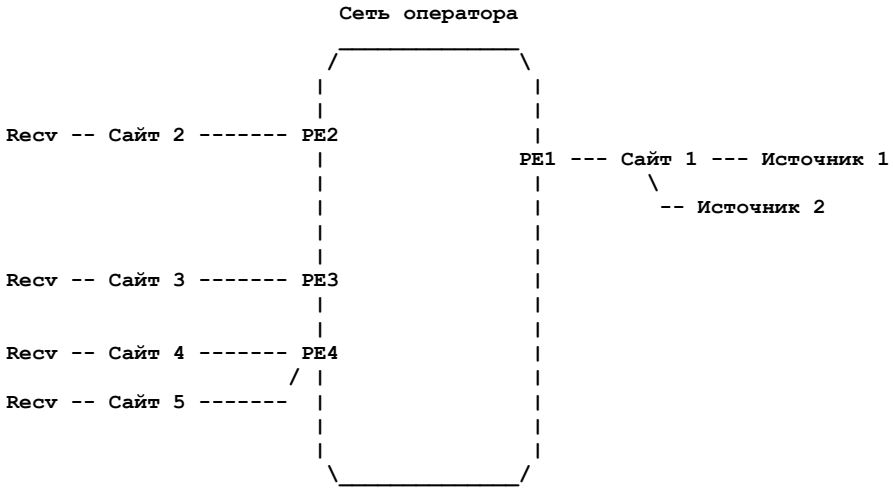

Рисунок 10. Пример услуг доставки кадров BUM.

Отображения multicast-групп на порты могут быть созданы с использованием листа rp-group-mappings. Поддерживается два метода отображения:

- статическая настройка групповых адресов Ethernet и портов (интерфейсов);
- протокол управления групповой адресацией на основе технологии L2, обеспечивающей сигнализацию сопоставления групповых адресов с портами (интерфейсами), такой как GARP[1]/GMRP[2] [IEEE-802-1D].

5.3. Обзор сайтов

Сайт представляет собой подключение площадки абонента к одной или множеству услуг VPN. Каждый сайт может быть связан с одной или несколькими площадками.

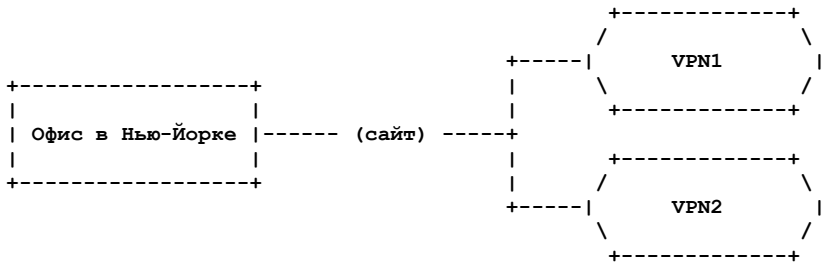

Рисунок 11. Офис абонента с двумя услугами VPN.

Провайдер использует контейнер site для хранения информации с подробным описанием соглашений с абонентом или операторами-партнерами для каждой точки присоединения (interconnect location).

Мы ограничиваем L2SM внешними интерфейсами (т. е. интерфейсами UNI и NNI), поскольку внутренние интерфейсы и базовая топология выходят за рамки L2SM.

Обычно в организации сервиса нужно документировать перечисленные ниже характеристики интерфейса сайта.

Уникальный идентификатор (site-id)
Произвольная строка, однозначно указывающая сайт в общей сетевой инфраструктуре. Формат site-id определяется локальным администратором сервиса VPN.

Устройство (device)
Абонент может запросить подключение одного или множества устройств CPE к SP для отдельного сайта.

Управление (management)
Определяет модель управления для сайта. Например, тип, транспорт системы управления, адрес. Эти параметры задают границу между SP и абонентом, т. е. владение устройством CE.

Местоположение (location)
Информация о месте расположения сайта, позволяющая легко отыскать данные о ближайших доступных ресурсах.

[1]Generic Attribute Registration Protocol - базовый протокол регистрации атрибутов.
[2]GARP Multicast Registration Protocol - протокол регистрации групп GARP.

Отличия сайта (site-diversity)

Представляет те или иные параметры для поддержки разнообразных сайтов.

Доступ сайта к сети (site-network-accesses)

Указывает список портов для сайта и их свойства, в частности параметры носителя (bearer), соединения и сервиса. Объект site-network-access представляет логическое соединение Ethernet для сайта. Сайт может иметь множество site-network-access.

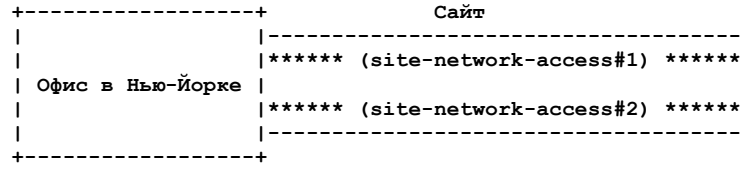

Рисунок 12. Два объекта Site-Network-Access для сайта.

Множество site-network-access используется, например, при многодомных подключениях и в некоторых других случаях.

Конфигурация сайта представляется глобальным элементом, предполагается, что роль системы управления заключается в разделении параметров между разными элементами внутри сети. Например, в случае конфигурации site-network-access система управления должна разделить параметры конфигурации между устройствами PE и CE.

Сайт может иметь однодомное или многодомное подключение. Во втором случае сайт может поддерживать множество site-network-access, в каждом из которых определяется элемент vpn-attachment (подключение к VPN), связывающий site-network-access с данным сайтом, а также указывающий сеть VPN, к которой сайт будет подключён.

5.3.1. Устройства и площадки

Информация в субконтейнере location контейнера site и в контейнере devices позволяет легко отыскать данные о ближайших доступных точках подключения и может применяться для планирования топологии доступа. Она может также использоваться другими компонентами оркестровки сети для выбора восходящего PE и нисходящего CE. Местоположение указывается в терминах почтовой адресации. Более подробные сведения о месте расположения можно указать с помощью дополнений.

Сайт может включать множество площадок и все такие площадки нужно указать в контейнере locations и списке. Типичным примером сайта с множеством площадок является центральный офис в городе, расположенный в нескольких зданиях. Эти здания могут размещаться в разных частях города и могут быть соединены внутригородскими оптическими линиями. Модель не представляет соединения между площадками сайта, поскольку они контролируются абонентом. В таких случаях при заказе услуг VPN абонент может запросить многодомное подключение в своих зданиях.

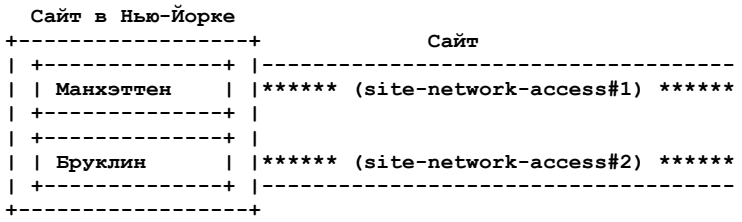

Рисунок 13. Два сайта, два Site-Network-Access.

Абонент может также запросить использование некоторых элементов оборудования (CE) у SP через контейнер devices. Для запрашиваемых CE предполагается управление со стороны провайдера или совместное управление. Может быть запрошено конкретное устройство для конкретной, уже включённой в конфигурацию площадки. Это позволит SP отправить устройство по указанному почтовому адресу. Для сайта с множеством площадок абонент может, например, запросить CE на каждую площадку, где требуется многодомное подключение. В примере на рисунке 13 одно устройство может быть запрошено для площадки на Манхэттене, другое - для площадки в Бруклине.

Используя контейнеры devices и locations, абонент может влиять на организацию многодомного подключения - одно устройство CE, два CE и т. д.

5.3.2. Доступ сайта в сеть

L2SM включает важный набор свойств физических интерфейсов и характеристик уровня Ethernet в контейнере site-network-accesses. Некоторые из них являются важными параметрами реализации, которые должны быть согласованы между абонентом и провайдером.

Как отмечено выше, сайт может быть многодомным. Каждое логическое подключение для сайта определяется контейнером site-network-accesses. Параметр site-network-access определяет способ подключения сайта к сети и включает три основных класса параметров:

- bearer определяет требования к подключению (ниже уровня L2);
- connection определяет параметры L2 для подключения;
- availability определяет политику доступности сайта в соответствии с определениями параграфа 5.8.

Параметр site-network-access имеет конкретный тип. Данный документ определяет 2 типа:

- point-to-point - соединение типа «точка-точка» между SP и абонентом;
- multipoint - многоточечное соединение между SP и абонентом.

Тип site-network-access может влиять на параметры, предлагаемые абоненту. Например, SP может не предлагать предоставление защиты от петель MAC при многоточечном доступе. Провайдер сам принимает решение о

поддерживаемых параметрах доступа для point-to-point и/или multipoint. Многоточечный доступ выходит за рамки документа. Некоторые контейнеры, определённые в этой модели, могут потребовать расширения для корректной работы при многоточечном доступе.

5.3.2.1. Контейнер bearer

Контейнер bearer определяет требования для подключения сайта (ниже уровня L2) к сети провайдера.

Параметры bearer помогают определить тип используемой для доступа среды передачи.

5.3.2.2. Контейнер connection

Контейнер connection определяет протокольные параметры L2 для подключения (например, vlan-id или circuit-id) и обеспечивают связность между абонентскими коммутаторами Ethernet. В зависимости от режима управления они относятся к адресации сегмента «PE-CE-ЛВС» или «CE-ЛВС абонента». В любом случае они описывают границу разделения ответственности между абонентом и провайдером. Для управляемого абонентом сайта параметры относятся к сегменту соединения «PE-CE-ЛВС», а для управляемого провайдером - к сегменту «CE-ЛВС абонента».

Параметр encapsulation-type позволяет абоненту выбрать инкапсуляцию Ethernet (доступ по портам) или Ethernet VLAN (доступ по VLAN). Все разрешённые типом интерфейса Ethernet (например, с тегами, без тегов, LAG) сервисные кадры могут быть указаны в ether-inf-type.

В соответствии с ether-inf-type контейнер connection представляет также три набора атрибутов канала для интерфейсов с тегами и без тегов, а также необязательного интерфейса LAG. Эти параметры важны для корректной организации соединения между устройствами CE и PE. Контейнер connection определяет также атрибут L2CP[1], обеспечивающий протокольное взаимодействие на уровне управления между устройствами CE и PE.

5.3.2.2.1. Интерфейс без тегов

Для каждого интерфейса без тегов (untagged-interface) имеются базовые параметры, такие как индекс и скорость, MTU, настройки автосогласования и управления потоком данных и т. п. В дополнение к этому на основе взаимного соглашения между абонентом и провайдером могут указываться дополнительные возможности - LLDP, IEEE 802.3ah [IEEE-802-3ah] или обнаружение/предотвращение петель MAC на интерфейсе UNI. Если требуется предотвращение петель, для атрибута uni-loop-prevention должно быть установлено значение true.

5.3.2.2.2. Интерфейс с тегами

Если на логическом модуле соединения для интерфейса включены услуги с тегами, в качестве encapsulation-type следует указывать инкапсуляцию Ethernet VLAN (при работе на основе VLAN) или VXLAN, а также следует установить в eth-inf-type индикацию использования тегов.

В дополнение к этому следует указать tagged-interface-type в контейнере tagged-interface для задания режима использования тегов. Текущая модель определяет пять режимов установки тегов VLAN:

- priority-tagged - SP инкапсулируют и помечают пакеты между CE и PE уровнем приоритета для кадра;
- dot1q-vlan-tagged - SP инкапсулируют пакеты между CE и PE с одним или множеством абонентских идентификаторов VLAN (CVLAN[2]);
- qinq - SP инкапсулируют пакеты на входе в свои сети с множеством идентификаторов CVLAN и одним тегом SP VLAN (SVLAN);
- qinany - SP инкапсулируют пакеты на входе в свои сети с неизвестными CVLAN и одним тегом SVLAN;
- vxlan - SP инкапсулирует пакеты на входе в свои сети и идентификатором VNI[3] и списком партнёров.

Общий S-tag для устройства Ethernet и (если применимо) отображение C-tag на SVC[4] помещаются в контейнер service. Для вариантов qinq и qinany значению S-tag в qinq и qinany в большинстве случаев следует соответствовать значению S-tag в контейнере service, однако в некоторых системах требуется трансляция VLAN для S-tag на обращённом наружу интерфейсе или восходящих PE для «нормализации» внешнего тега VLAN в S-tag сервиса на входе в сеть и обратной трансляции в S-tag при выходе из сети. Одним из примеров является агрегирующий коммутатор L2 на пути - S-tag для SVC ранее был назначен другому сервису и не может использоваться этим AC.

5.3.2.2.3. Интерфейс LAG

Иногда абонентам может потребоваться сборка множества физических каналов в одно логическое соединение LAG (точка-точка) с SP. Обычно на таких соединения применяется протокол LACP[5] для динамического добавления или удаления каналов в группу-агрегат. В общем случае LAG позволяет расширить пропускную способность сервиса по сравнению с одиночным каналом, обеспечивая аккуратное снижение пропускной способности при отказе канала в группе, а также повышение уровня доступности.

В L2SM имеется набор атрибутов (под lag-interface), связанных с агрегированием каналов. Абонент и провайдер сначала должны решить, будет ли выполняться обмен LACP PDU между краевыми устройствами, и выбрать для LACP-state значение on или off. При включённом протоколе LACP обе стороны должны указать, (1) будет LACP работать в пассивном или активном режиме и (2) задать временной интервал и уровень приоритета для LACP PDU. Абонент и провайдер могут также определить минимальную пропускную способность агрегата LAG, которая считается допустимой, путём задания необязательного атрибута mini-link-num. Для включения быстрого детектирования отказов на каналах через независимые сессии UDP работает микро-BFD[6] [RFC7130] для мониторинга состояния каждого канала в группе. Абоненту и провайдеру следует согласовать интервал BFD hello и время удержания.

---

[1] Layer 2 Control Protocol - канал управления L2.
[2] Customer VLAN.
[3] VXLAN Network Identifier.
[4] Switched Virtual Circuit - коммутрируемое виртуальное устройство.
[5] Link Aggregation Control Protocol - протокол управления агрегированием каналов.
[6] Bidirectional Forwarding Detection - двухстороннее детектирование пересылки.

Каждый канал группы указывается под интерфейсом LAG с базовыми свойствами физического канала. Некоторые атрибуты, такие как управление потоком данных, тип инкапсуляции, разрешённые Ethertype на входе и установки LLDP задаются на уровне LAG.

5.3.2.2.4. Отображение CVLAN-ID на SVC

Когда более одного сервиса мультиплексируется в один интерфейс, входящие кадры передаются в один из экземпляров сервиса L2VPN в соответствии с заранее согласованным сопоставлением абонентских VLAN с SVC. Множество CVLAN может передаваться через один канал SVC. Тип группировки будет определять связывание множества CVLAN в одном экземпляре сервиса VPN (т. е. группировку VLAN).

Когда это применимо, отображение cvlan-id-to-svc-map содержит список CVLAN, отображённых на один сервис. В большинстве случаев это будет списком доступа по VLAN из внутреннего тега 802.1Q [IEEE-802-1Q] (C-tag).

Сервис VPN можно настроить на сохранение CE-VLAN ID и CE-VLAN CoS от сайта-источника до сайта-получателя. Это нужно в тех случаях, когда абонент хочет использовать информацию из заголовка VLAN на обоих сайтах. Сохранение CE-VLAN ID и CE-VLAN CoS применяется в каждом site-network-access на сайтах. Это сохранение означает, что CE-VLAN ID и/или CE-VLAN CoS на стороне отправителя должны совпадать со значениями этих полей на стороне сайта-получателя, относящегося к тому же сервису L2VPN.

Если разрешена группировка для всех сайтов (тип группировки all-to-one), сохранение применяется для всех входящих кадров сервиса. Если группировка не включена, сохранение применяется для входящих кадров с тегом CE-VLAN ID.

5.3.2.2.5. Поддержка управления L2CP

Абоненту и SP следует заранее согласовать вопрос разрешения протокольных взаимодействий между CE и PE на уровне управления. Для обеспечения эффективной доставки группового трафика абоненты могут применять протоколы управления Ethernet (например, STP[1] [IEEE-802-1D]).

Для поддержки эффективной динамической доставки могут использоваться кадры управления групповой передачей Ethernet (например, GARP/GMRP [IEEE-802-1D]) между устройствами CE и PE. Однако **недопустимо** предполагать, что все CE всегда используют такие протоколы (например, CE может быть маршрутизатором или не знать деталей L2).

MAC-адреса получателей в L2CP PDU относятся к двум резервным блокам, заданным рабочей группой IEEE 802.1. Для пакетов с MAC-адресом получателя из указанных ниже групповых диапазонов применяются особые правила пересылки.

- Протоколы мостов - 01-80-C2-00-00-00 - 01-80-C2-00-00-0F.
- Протоколы MRP - 01-80-C2-00-00-20 - 01-80-C2-00-00-2F.

Туннелирование протоколов L2 позволяет SP передавать абонентские L2 PDU через сеть без интерпретации и обработки на промежуточных устройствах. Эти L2CP PDU инкапсулируются с использованием QinQ для передачи через ядро сети с поддержкой MPLS.

Контейнер L2CP-control содержит список обычно используемых протоколов и параметров L2CP. SP может задать для каждого отдельного протокола режим отбрасывания (discard-mode), партнёрства (peer-mode) или туннелирования (tunnel-mode).

5.3.2.2.6. Ethernet Service OAM

Применение Ethernet в качестве технологии распределенных сетей предъявляет дополнительные требования к сквозному мониторингу сервиса и контролю отказов в сетях SP, особенно в части доступности сервиса и среднего времени восстановления (MTTR[2]). Ethernet Service OAM в контексте L2SM означает комбинацию протоколов IEEE 802.1ag [IEEE-802-1ag] и ITU-T Y.1731 [ITU-T-Y-1731].

Вообще говоря, Ethernet Service OAM позволяет SP проверять непрерывность предоставления услуг, изолировать отказы, измерять задержки и их вариации на уровне абонента и доступа сайта в сеть. Информация Ethernet Service OAM дополняет данные других инструментов верхних уровней IP/MPLS OSS для обеспечения SLA.

Функциональная модель обработки отказов 802.1ag CFM[3] структурирована в иерархические домены MD[4], каждому из которых назначается уникальный уровень обслуживания. MD верхних уровней могут быть вложены в MD нижних уровней, однако домены MD не могут пересекаться. Область действия каждого домена MD полностью находится в сети абонента или сети SP. Домены MD могут взаимодействовать между CE и PE (от абонента к провайдеру) или между PE (взаимодействие провайдеров), а также могут туннелироваться через другую сеть SP.

В зависимости от варианта применения несколько точек MEP[5] может размещаться на обращённом наружу интерфейсе, передавая CFM PDU в направлении ядра сети (Up MEP) или в нисходящий канал (Down MEP).

Субконтейнер cfm-802.1-ag в контейнере site-network-access представляет ассоциацию обслуживания CFM MA[6], т. е. Down MEP для UNI MA. Для каждой ассоциации MA пользователь может задать идентификатор MAID[7], уровень и направление MEP, Remote MEP ID, уровень CoS для CFM PDU, интервал и время удержания сообщений проверки связности (CCM[8]), уровень генерации сигналов об отказе (т. е. самый низкий приоритет, при котором генерируется сигнал об отказе), тип приоритета CCM и т. п.

[1] Spanning Tree Protocol - протокол связующего дерева.
[2] Mean Time To Repair.
[3] Connectivity Fault Management - обработка отказов в соединениях.
[4] Maintenance Domain - домен обслуживания.
[5] Maintenance Entity Group End Point - конечная точка группы объектов обслуживания.
[6] Maintenance Association.
[7] Maintenance Association Identifier.
[8] Continuity Check Message.

Мониторинг производительности ITU-T Y.1731 (PM[1]) обеспечивает важную телеметрическую информацию, которая включает задержку кадров Ethernet и её вариации, потери кадров и пропускную способность для кадров. Измерения задержки и её вариаций могут выполняться в одном или обоих направлениях. Обычно зонд Y.1731 PM передаёт небольшое число синтетических кадров вместе с обычными кадрами для измерения параметров SLA.

Субконтейнер y-1731 в контейнере site-network-access содержит набор данных для определения параметров зонда PM, включая MAID, локальный и удалённый идентификатор MEP ID, тип PM PDU, период сообщений и интервал измерения, уровень CoS для PM PDU, опции измерения по синтетическим или естественным кадрам, одно или два направления для измерений, размер кадров PM и тип сессии.

5.4. Роли сайта

Сервис VPN имеет определённую топологию, как описано в параграфе 5.2.2. В результате каждому сайту, относящемуся к VPN, назначается в этой топологии определённая роль. Лист site-role указывает роль сайта в конкретной топологии VPN.

В топологии any-to-any (каждый с каждым) все сайты **должны** играть одну роль - any-to-any-role.

В топологии Hub-and-Spoke или Hub-and-Spoke-Disjoint сайты **должны** играть роль Hub или Spoke.

5.5. Сайты, входящие в несколько VPN

5.5.1. Варианты VPN на сайте

Сайт может входить в одну или множество сетей VPN и site-vpn-flavor указывает способ мультиплексирования VPN. Возможны 4 типа обращённых наружу соединений, связанных с сервисом EVPN и сайтом. Поэтому модель поддерживает четыре варианта:

- site-vpn-flavor-single - сайт входит в единственную сеть VPN;
- site-vpn-flavor-multi - сайт включён во множество VPN и все логические соединения сайтов относятся к одному набору VPN;
- site-vpn-flavor-nni - сайт представляет интерфейс NNI, где соединяются два административных домена, относящихся к одному или разным провайдерам;
- site-vpn-flavor-e2e - сайт представляет сквозное многосегментное соединение.

5.5.1.1. Одно подключение - site-vpn-flavor-single

На рисунке 14 показано подключение сайта к одной сети VPN.

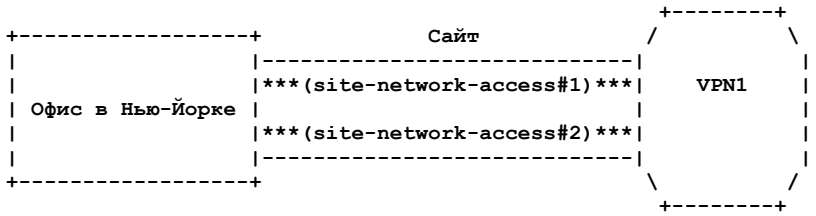

Рисунок 14. Одно подключение к VPN.

5.5.1.2. Множество подключений - site-vpn-flavor-multi

На рисунке 15 показано подключение сайта к множеству VPN.

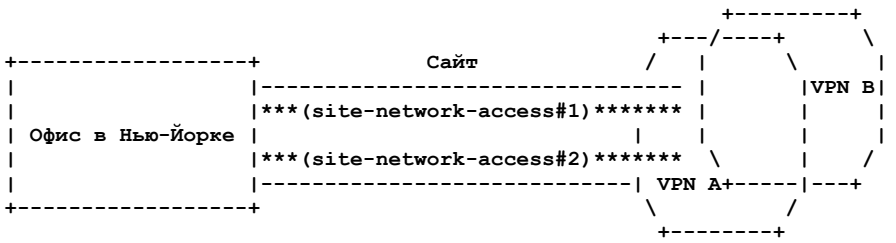

Рисунок 15. Подключение к множеству VPN.

Офис в Нью-Йорке на рисунке 15 является многодомным. Для обоих логических соединений применяются одинаковые правила подключения к VPN и оба соединения относятся к VPN A и VPN B.

Доступ к VPN A или VPN B из офиса в Нью-Йорке выполняется на основе пересылки по MAC-адресу получателя. Возможность доступа к одному адресату из двух VPN может создавать проблемы маршрутизации. В этом случае роль администратора абонентской сети заключается в подходящем отображении MAC-адресов каждой VPN. Более подробное описание приведено в параграфах 5.5.2 и 5.10.2, а поддержка BUM рассмотрена в параграфе 5.10.3.

5.5.1.3. NNI - site-vpn-flavor-nni

Вариант с межсетевым соединением (NNI) можно промоделировать, используя контейнер sites. Для SP полезно указать, что запрашиваемое соединение VPN не относится к обычному сайту, а является NNI, поскольку в этом случае могут по умолчанию применяться другие параметры конфигурации (например, ACL[2], правила маршрутизации).

На рисунке 16 показан вариант A сценария NNI, который можно смоделировать с помощью контейнера sites. Для подключения абонентских VPN (VPN1 и VPN2) к сети SP B провайдер SP A может запросить создание того или иного

[1]Performance Monitoring.
[2]Access Control List - список контроля доступа.

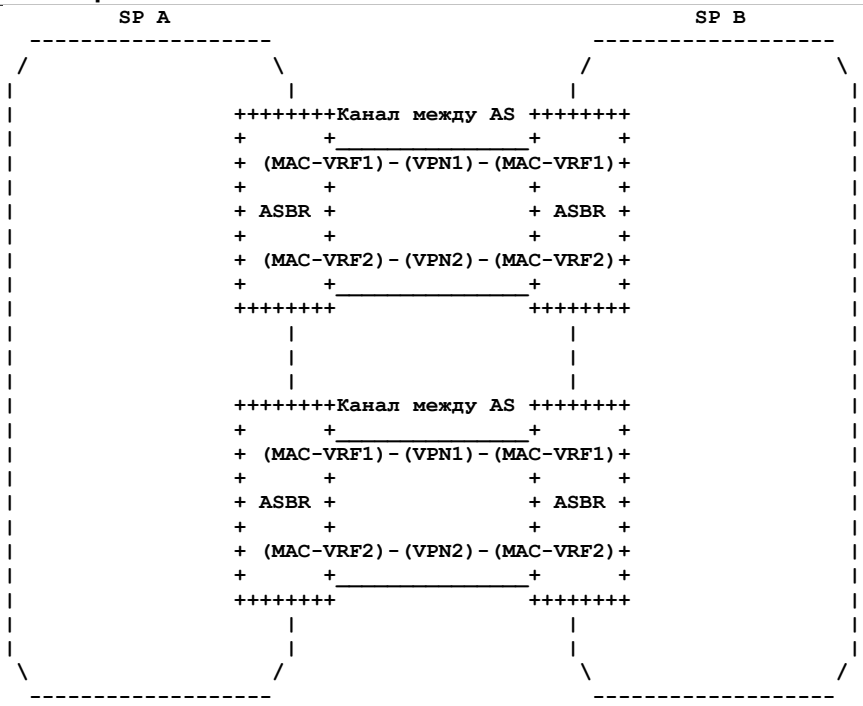

Рисунок 16. Сценарий NNI, вариант A.

контейнера site-network-accesses для сети SP B. Можно использовать тип site-vpn-flavor-nni для информирования SP B о том, что это соединение NNI, а не обычное подключение абонента.

5.5.1.4. E2E - site-vpn-flavor-e2e

Сквозное (E2E[1]) многосегментное соединение VPN организуется из нескольких соединительных сегментов. Для SP будет полезно указать, что запрошенное соединение VPN не является обычным подключением сайта, а служит сквозным соединением VPN, поскольку в случае site-vpn-flavor-e2e по умолчанию могут применяться другие параметры (например, конфигурация QoS). Для организации соединения между Сайтом 1 в SP A и Сайтом 2 в SP B через множество доменов провайдер SP A может запросить организацию сквозного соединения с SP B. Тип site-vpn-flavor-e2e позволяет указать, что это сквозное соединение, а не обычное подключение абонентского сайта.

5.5.2. Присоединение сайта к VPN

По причине наличия множества вариантов site-vpn присоединение сайта к L2VPN выполняется на уровне site-network-access (логический доступ) через контейнер vpn-attachment, который является обязательным. Модель обеспечивает два способа присоединения сайта к VPN:

- по непосредственной ссылке на целевую сеть VPN;
- по ссылке на правила присоединения к VPN, которые могут быть более сложными.

Эти опции позволяют пользователю выбрать наиболее подходящий вариант.

5.5.2.1. Указание VPN

Указание vpn-id обеспечивает простой способ привязать конкретное логическое соединение к VPN. Это является лучшим способом для VPN с одним подключением. При указании vpn-id должна добавляться роль сайта (site-role) в топологии целевого сервиса VPN.

```
<?xml version="1.0"?>
<l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
 <vpn-services>
    <vpn-service>
      <vpn-id>VPNA</vpn-id>
      <ce-vlan-preservation>true</ce-vlan-preservation>
      <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
    </vpn-service>
    <vpn-service>
      <vpn-id>VPNB</vpn-id>
      <ce-vlan-preservation>true</ce-vlan-preservation>
      <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
    </vpn-service>
 </vpn-services>
 <sites>
   <site>
    <site-id>SITE1</site-id>
   <locations>
    <location>
     <location-id>L1</location-id>
    </location>
   </locations>
   <management>
    <type>customer-managed</type>
```

[1]End-to-end.

```
          </management>
           <site-network-accesses>
            <site-network-access>
             <network-access-id>LA1</network-access-id>
                <service>
                  <svc-bandwidth>
                     <bandwidth>
                       <direction>input-bw</direction>
                        <type>bw-per-cos</type>
                         <cir>450000000</cir>
                         <cbs>20000000</cbs>
                         <eir>1000000000</eir>
                         <ebs>200000000</ebs>
                     </bandwidth>
                    </svc-bandwidth>
                     <carrierscarrier>
                       <signaling-type>bgp</signaling-type>
                     </carrierscarrier>
                     <svc-mtu>1514</svc-mtu>
                   </service>
            <vpn-attachment>
             <vpn-id>VPNA</vpn-id>
             <site-role>spoke-role</site-role>
            </vpn-attachment>
           </site-network-access>
           <site-network-access>
            <network-access-id>LA2</network-access-id>
                <service>
                  <svc-bandwidth>
                     <bandwidth>
                       <direction>input-bw</direction>
                        <type>bw-per-cos</type>
                         <cir>450000000</cir>
                         <cbs>20000000</cbs>
                         <eir>1000000000</eir>
                         <ebs>200000000</ebs>
                     </bandwidth>
                    </svc-bandwidth>
                     <carrierscarrier>
                       <signaling-type>bgp</signaling-type>
                     </carrierscarrier>
                     <svc-mtu>1514</svc-mtu>
                   </service>
            <vpn-attachment>
             <vpn-id>VPNB</vpn-id>
             <site-role>spoke-role</site-role>
            </vpn-attachment>
           </site-network-access>
          </site-network-accesses>
      </site>
     </sites>
    </l2vpn-svc>
```

Приведенный выше пример описывает случай множества VPN, где сайт (SITE1) имеет два логических подключения (LA1 и LA2) к сетям VPNA и VPNB.

5.5.2.2. Политика VPN

Список vpn-policy позволяет описать вариант с множеством VPN, где логические подключения относятся к разным VPN.

Поскольку сайт может входить в несколько VPN, список vpn-policy может включать множество записей. Можно использовать фильтр для выбора ЛВС на сайте, которые будут частью определённой сети VPN. Сайт может включать множество сегментов ЛВС, каждый из которых может быть подключён к своей сети VPN. Каждый раз при подключении сайта (или ЛВС) к VPN пользователь должен точно указать его роль (site-role) в топологии целевого сервиса VPN.

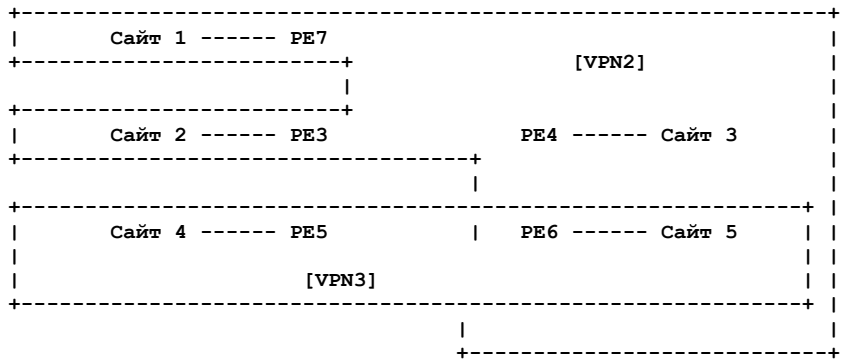

Рисунок 17. Пример политики VPN.

На рисунке 17 Сайт 5 входит в VPN3 и VPN2, выступая в качестве Hub для VPN2 и any-to-any для VPN3. Этот вариант подключения описан ниже.

```
<?xml version="1.0"?>
 <l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
  <vpn-services>
```

```
      <vpn-service>
       <vpn-id>VPN2</vpn-id>
       <ce-vlan-preservation>true</ce-vlan-preservation>
       <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
      </vpn-service>
      <vpn-service>
       <vpn-id>VPN3</vpn-id>
       <ce-vlan-preservation>true</ce-vlan-preservation>
       <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
      </vpn-service>
     </vpn-services>
     <sites>
        <site>
       <locations>
        <location>
         <location-id>L1</location-id>
        </location>
       </locations>
       <management>
        <type>customer-managed</type>
       </management>
          <site-id>Site5</site-id>
          <vpn-policies>
           <vpn-policy>
            <vpn-policy-id>POLICY1</vpn-policy-id>
            <entries>
             <id>ENTRY1</id>
             <vpn>
              <vpn-id>VPN2</vpn-id>
              <site-role>hub-role</site-role>
             </vpn>
            </entries>
            <entries>
             <id>ENTRY2</id>
             <vpn>
              <vpn-id>VPN3</vpn-id>
              <site-role>any-to-any-role</site-role>
             </vpn>
            </entries>
           </vpn-policy>
          </vpn-policies>
          <site-network-accesses>
           <site-network-access>
            <network-access-id>LA1</network-access-id>
         <site>
          <site-id>SITE1</site-id>
       <locations>
        <location>
         <location-id>L1</location-id>
        </location>
       </locations>
       <management>
        <type>customer-managed</type>
       </management>
          <site-network-accesses>
           <site-network-access>
            <network-access-id>LA1</network-access-id>
                <service>
                  <svc-bandwidth>
                     <bandwidth>
                       <direction>input-bw</direction>
                        <type>bw-per-cos</type>
                         <cir>450000000</cir>
                         <cbs>20000000</cbs>
                         <eir>1000000000</eir>
                         <ebs>200000000</ebs>
                     </bandwidth>
                   </svc-bandwidth>
                    <carrierscarrier>
                      <signaling-type>bgp</signaling-type>
                    </carrierscarrier>
                    <svc-mtu>1514</svc-mtu>
                 </service>
           <vpn-attachment>
            <vpn-id>VPNA</vpn-id>
            <site-role>spoke-role</site-role>
           </vpn-attachment>
          </site-network-access>
          <site-network-access>
           <network-access-id>LA2</network-access-id>
                <service>
                  <svc-bandwidth>
                     <bandwidth>
                       <direction>input-bw</direction>
                        <type>bw-per-cos</type>
                         <cir>450000000</cir>
```

```
                    <cbs>20000000</cbs>
                    <eir>1000000000</eir>
                    <ebs>200000000</ebs>
                  </bandwidth>
                 </svc-bandwidth>
                  <carrierscarrier>
                    <signaling-type>bgp</signaling-type>
                  </carrierscarrier>
                  <svc-mtu>1514</svc-mtu>
                </service>
          <vpn-attachment>
           <vpn-id>VPNB</vpn-id>
           <site-role>spoke-role</site-role>
          </vpn-attachment>
         </site-network-access>
        </site-network-accesses>
       </site>
          <vpn-attachment>
           <vpn-policy-id>POLICY1</vpn-policy-id>
          </vpn-attachment>
         </site-network-access>
        </site-network-accesses>
       </site>
  </sites>
</l2vpn-svc>
```

Если требуется более детальное управление подключением к VPN, можно воспользоваться фильтрацией. Например, если сеть LAN1 Сайта 5 должна быть подключена к VPN2 в роли Hub, а LAN2 должна быть подключена к VPN3, можно использовать приведённую ниже конфигурацию.

```
<?xml version="1.0"?>
  <l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
    <vpn-services>
      <vpn-service>
        <vpn-id>VPN2</vpn-id>
        <ce-vlan-preservation>true</ce-vlan-preservation>
        <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
        </vpn-service>
        <vpn-service>
         <vpn-id>VPN3</vpn-id>
         <ce-vlan-preservation>true</ce-vlan-preservation>
         <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
        </vpn-service>
    </vpn-services>
  <sites>
   <site>
   <locations>
    <location>
     <location-id>L1</location-id>
    </location>
   </locations>
   <management>
    <type>customer-managed</type>
   </management>
         <site-id>Site5</site-id>
         <vpn-policies>
          <vpn-policy>
           <vpn-policy-id>POLICY1</vpn-policy-id>
           <entries>
            <id>ENTRY1</id>
            <filters>
              <filter>
                <type>lan</type>
                <lan-tag>LAN1</lan-tag>
              </filter>
            </filters>
            <vpn>
             <vpn-id>VPN2</vpn-id>
             <site-role>hub-role</site-role>
            </vpn>
           </entries>
           <entries>
            <id>ENTRY2</id>
            <filters>
              <filter>
                <type>lan</type>
                <lan-tag>LAN2</lan-tag>
              </filter>
            </filters>
             <vpn>
             <vpn-id>VPN3</vpn-id>
             <site-role>any-to-any-role</site-role>
            </vpn>
           </entries>
          </vpn-policy>
         </vpn-policies>
         <site-network-accesses>
```

```
            <site-network-access>
             <network-access-id>LA1</network-access-id>
               <service>
                 <svc-bandwidth>
                    <bandwidth>
                     <direction>input-bw</direction>
                      <type>bw-per-cos</type>
                       <cir>450000000</cir>
                       <cbs>20000000</cbs>
                       <eir>1000000000</eir>
                       <ebs>200000000</ebs>
                    </bandwidth>
                  </svc-bandwidth>
                   <carrierscarrier>
                      <signaling-type>bgp</signaling-type>
                   </carrierscarrier>
                    <svc-mtu>1514</svc-mtu>
                </service>
             <vpn-attachment>
              <vpn-policy-id>POLICY1</vpn-policy-id>
             </vpn-attachment>
            </site-network-access>
           </site-network-accesses>
          </site>
         </sites>
        </l2vpn-svc>
```

5.6. Определение точки подключения сайта

Система управления будет определять для каждого site-network-access на конкретном сайте точку подключения к сети провайдера (например, PE или агрегирующий коммутатор).

Эта модель определяет параметры и ограничения, которые могут влиять на подключение site-network-access.

Система управления **должна** соблюдать все ограничения абонента, а если ограничения слишком жесткие и не могут быть выполнены, системе управления **недопустимо** подключать сайт и пользователю **должна** передаваться информация о всех ограничениях, которые не могут быть выполнены. Предоставление такой информации выходит за рамки документа. Вопрос ослабления заданных ограничений решается пользователем.

Параметры расположения сайта (параграф 5.6.2) и типа доступа (параграф 5.6.3) влияют на размещение сервиса, выбираемое системой управления.

Кроме учёта параметров и ограничений на решение системы управления **могут** влиять внутренние ограничения SP, например, наименьшая загрузка или удалённость.

5.6.1. Ограничение - устройство

При управлении со стороны провайдера или совместном управлении абонент может заказать одно или множество устройств на конкретную площадку, которая уже настроена. Абонент может принудительно задать site-network-access для подключения заказанного устройства.

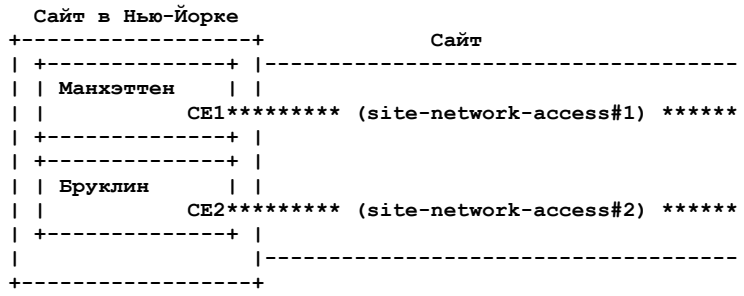

Рисунок 18. Пример ограничений для устройства.

На рисунке 18 site-network-access#1 связывается с устройством CE1 из запроса. SP должен обеспечить это подключение.

5.6.2. Ограничение и параметр - расположение сайта

Обеспечивая этой моделью информация о местоположении **может** применяться системой управления при поиске PE для подключения сайта (на стороне SP). С каждым подключением сайта к сети должно быть связано конкретное место. Провайдер **должен** обеспечивать завершение сервиса в указанной точке доступа сайта в сеть (на стороне абонента). Значение country-code в местоположении сайта следует указывать кодом ISO 3166 и оно похоже на метку country, определённую в [RFC4119].

Местоположение site-network-access определяется значением location-flavor. Для сайтов, управляемых провайдером или совместно с ним, предполагается, что пользователь укажет значение device-reference (для устройства), которое свяжет site-network-access с конкретным устройством, заказанным абонентом. Поскольку устройство связано с конкретным местом, в этом случае информация о местоположении определяется по размещению устройства. Если сайт управляется абонентом, предполагается, что пользователь укажет location-reference (для местоположения) и это значение будет указывать уже настроенное местоположение, что поможет в размещении.

На рисунке 19 управляемый абонентом Сайт 1 имеет местоположение L1, а для управляемого провайдером Сайта 2 заказано устройство CE (CE#1). Для Сайта 2 указано местоположение L2. При настройке site-network-access для Сайта 1 пользователь должен указать местоположение L1, чтобы система управления знала, что в этом месте организуется

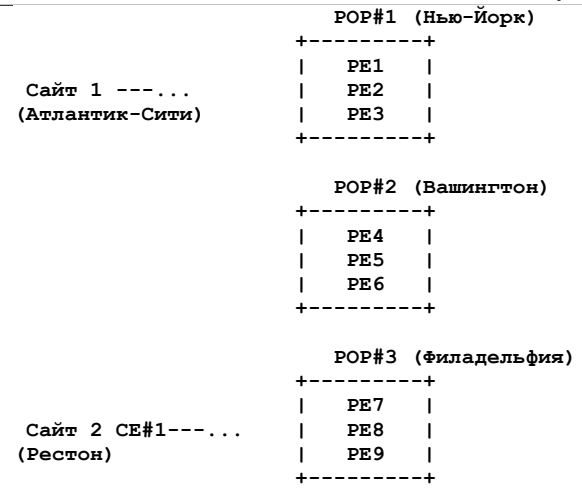

Рисунок 19. Данные о местоположении сайтов.

доступ. Затем с учётом расстояния система управления может соединить Сайт 1 с PE в Philadelphia POP. При этом могут также учитываться ресурсы, доступные на PE, для точного определения целевого устройства PE (например, менее загруженного). Для Сайта 2 предполагается, что пользователь настроит site-network-access со ссылкой (device-reference) на CE#1, чтобы система управления знала о том, что доступ будет завершаться в месте размещения устройства CE#1, которое должно быть подключено. Для организации подключения на стороне SP в случае использования ближайшего PE, Сайт 2 может быть подключён к Washington POP.

5.6.3. Ограничение и параметр - тип доступа

Система управления должна выбрать среду для подключения сайта (например, xDSL, арендованная линия, Ethernet). Абонент может задать некоторые параметры и/или ограничения, которые помогут системе управления выбрать среду.

Информацию контейнера bearer **следует** рассматривать в первую очередь.

- Параметр requested-type обеспечивает информацию о типе среды, который абонент хочет использовать. Если лист strict имеет значение true, система управления **должна** считать это строгим ограничением для типа среды. Если strict = false (принято по умолчанию) и запрошенная среда недоступна, система управления может выбрать другой тип среды. Абоненту и провайдеру **следует** обменяться данными о поддерживаемых типах сред, но механизмы такого обмена выходят за рамки документа.
- Лист always-on определяет строгое ограничение. При значении true система управления **должна** выбрать тип среды, которая всегда доступна (always-on), т. е. не может применяться коммутируемый доступ.
- Параметр bearer-reference используется в тех случаях, когда абонент уже заказал подключение к сети SP отдельно от сайта L2VPN и хочет воспользоваться этим соединением. Строка служит внутренней ссылкой от SP и описывает уже имеющееся соединение. Это требование является строгим и не может быть ослаблено. Способ предоставления ссылки абоненту выходит за рамки документа, но примером может служить указание канала-носителя, заказанного клиентом (с помощью процедуры, выходящей за рамки документа).

Могут применяться также иные внутренние параметры от SP. Система управления **может** использовать такие параметры, как «input svc-bandwidth» и «output svc-bandwidth» для выбора используемого типа доступа.

5.6.4. Ограничение - разнесение доступа

Каждый элемент site-network-access может включать одно или множество ограничений, которые будут определять размещение доступа. По умолчанию в модели предполагается отсутствие ограничений, но ожидается выделение уникального носителя (bearer) для каждого site-network-access.

Для реализации разных вариантов доступа элементы site-network-access можно помечать с помощью одного или нескольких идентификаторов групп. Идентификатор группы представляет собой строку, которая может включать как явное именование группы сайтов (например, multihomed-set1), так и числовое значение (например, 12345678). Значение каждого group-id локально для администратора абонента и система управления **должна** обеспечивать разным абонентам возможность использования одинаковых идентификаторов. Один или несколько group-id могут быть также определены на уровне сайта, в результате чего все site-network-access этого сайта **должны** наследовать идентификаторы group-id своего сайта. Когда в дополнение group-id сайта определяются идентификаторы на уровне site-network-access, система управления **должна** учитывать объединение всех групп (уровня сайта и уровня site-network-access) для конкретного элемента site-network-access.

Для уже настроенного элемента site-network-access каждое ограничение **должно** быть выражено применительно к набору site-network-accesses. Уже настроенный элемент site-network-access **должен** не приниматься во внимание в целевом наборе site-network-accesses. Например, «site-network-access S недопустимо подключать к той же точке присутствия POP, куда подключён контейнер site-network-accesses, являющийся частью Group 10». Набор site-network-accesses, к которому применяются ограничения, может быть указан в форме списка групп all-other-accesses или all-other-groups. Опция all-other-accesses означает, что текущее ограничение site-network-access допустимо применять ко всем site-network-accesses, относящимся к текущему сайту. Опция all-other-groups означает, что ограничение **должно** применяться ко всем группам, в которые текущий элемент site-network-access не входит.

Текущая модель определяет множество типов ограничений, перечисленных ниже.

- pe-diverse - текущий элемент site-network-access **недопустимо** соединять с тем же PE, что и целевой site-network-accesses.

- pop-diverse - текущий элемент site-network-access **недопустимо** соединять с той же точкой POP, что и целевой site-network-accesses.
- linecard-diverse - текущий элемент site-network-access **недопустимо** соединять с той же линейной платой, что и целевой site-network-accesses. Отметим, что абонент может запросить linecard-diverse для site-network-accesses, но идентификатор текущей используемой линейной платы не следует показывать абоненту.
- bearer-diverse - текущему элементу site-network-access **недопустимо** использовать общие компоненты носителя (bearer) с носителями, используемыми целевым site-network-accesses. Элемент bearer-diverse обеспечивает некоторый уровень разнесения доступа. Например, двум bearer-diverse site-network-accesses недопустимо использовать один мультиплексор DSLAM[1], BAS[2] или коммутатор L2.
- same-pe - текущий элемент site-network-access **должен** соединяться с тем же PE, что и целевой site-network-accesses.
- same-bearer - текущий элемент site-network-access **должен** соединяться с тем же носителем, что и целевой site-network-accesses.

Типы ограничений могут быть расширены с помощью дополнений. Каждое ограничение должно выражаться в форме «элемент site-network-access S должен быть <constraint-type> (например, pe-diverse, pop-diverse) из <target> site-network-accesses».

Идентификатор group-id, используемый для нацеливания того или иного site-network-accesses, может совпадать с применяемым в текущем элементе site-network-access. Это упрощает настройку для случаев, где группа точек site-network-access имеет ограничения между собой.

5.7. Выделение значений RD

Обозначение маршрута (RD[3]) является важнейшим параметром L2VPN на основе протокола BGP, описанных в [RFC4364], который обеспечивает возможность различать общие блоки адресов в разных VPN. Поскольку для целей маршрутов (RT) предполагается выделение системой управления таблиц MAC-VRF на целевом PE и RD для этих MAC-VRF, значение RD **должно** быть уникальным для каждой таблицы MAC-VRF в целевом PE.

Если MAC-VRF уже есть в целевом PE и удовлетворяет ограничениям для сайта, нет необходимости создавать другую таблицу MAC-VRF и сайт **может** быть подключён с использованием имеющейся MAC-VRF. Проверка системой управления соответствия имеющейся MAC-VRF ограничениям для сайта выходит за рамки документа.

Если таблицы MAC-VRF нет в целевом PE, система управления инициирует создание MAC-VRF в целевом PE и выделение для неё нового значения RD.

Система управления **может** применять политику выделения RD на уровне VPN или MAC-VRF в зависимости от правил SP. При выделении на уровне VPN все таблицы MAC-VRF (отправленные в разные PE) в рамках VPN будут использовать общее значение RD. При выделении на уровне MAC-VRF каждой таблице MAC-VRF следует назначать уникальное значение RD. Возможны другие варианты выделения значений и данный документ не ограничивает выбор.

Выделение RD **может** выполняться таким же способом как для RT. Представленная в параграфе 5.2.2.1 информация пригодна и в этом случае.

Отметим, что SP **может** настроить целевое устройство PE на автоматическое выделение значений RD. В таких случаях не потребуется какой-либо отдельной системы (backend) для назначения RD.

5.8. Доступность Site-Network-Access

Сайт может быть многодомным с множеством точек site-network-access. Ограничения на размещение, описанные в параграфе 5.6, помогут обеспечить разнесение физических подключений.

При размещении site-network-accesses в сети абонент может захотеть использовать определённую политику маршрутизации для этого доступа. Контейнер site-network-access/availability определяет параметры избыточности для резервирования на данном сайте. Лист access-priority определяет предпочтения для конкретного доступа. Эти предпочтения используются в сценариях «основной-резервный» и «распределение нагрузки». Большее значение access-priority задаёт более предпочтительное использование. Атрибут redundancy-mode определён для многодомных сайтов и служит для использования в сценариях «один активный» и «активный-активный». Это позволяет поддерживать множество активных путей в состоянии пересылки и для распределения нагрузки.

На рисунке 20 показаны варианты использования атрибута access-priority.

Для ЛВС Hub#2 требуется распределение нагрузки, поэтому оба site-network-access должны иметь одинаковые значения access-priority. Для ЛВС Hub#1 требуется резервирование доступа и большее значение access-priority определяет основное соединение (site-network-access).

[1]Digital Subscriber Line Access Multiplexer - мультиплексор цифровых абонентских линий доступа.
[2]Broadband Access Switch - коммутатор широкополосного доступа.
[3]Route Distinguisher.

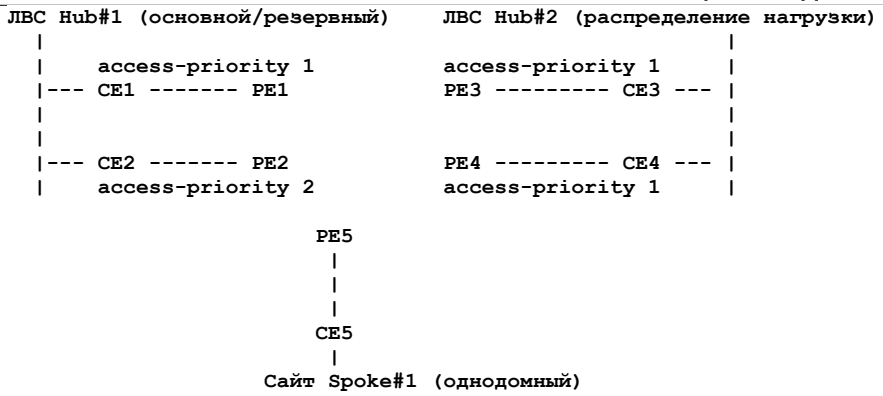

Рисунок 20. Пример настройки приоритета доступа.

Могут быть промоделированы и более сложные сценарии. Рассмотрим Hub-сайт с 5 подключениями к сети (A1, A2, A3, A4, A5). Абонент хочет в обычных условиях распределять нагрузку между соединениями A1 и A2, при отказе этих каналов - распределять нагрузку между A3 и A4, а случае отказа всех каналов A1, A2, A3 и A4 - использовать канал A5. Это можно реализовать, установив значения access-priority: A1=100, A2=100, A3=50, A4=50, A5=10.

Подход access-priority имеет некоторые ограничения. Например, в описанном выше случае переход на распределение нагрузки между каналами A3 и A4 недостижим в случае отказа лишь одного из каналов A1 и A2. Однако атрибут access-priority хорошо подходит для большинства практических реализаций и при необходимости модель может быть расширена с помощью дополнений.

5.9. SVC MTU

Значение MTU для кадров абонентского сервиса можно вывести из принятого по умолчанию MTU физических интерфейсов или задать в листе svc-mtu, если принятое по умолчанию значение не подходит.

5.10. Контейнер service

Контейнер service определяет параметры сервиса, связанные с сайтом.

5.10.1. Параметр Bandwidth

Параметр bandwidth указывает требования к пропускной способности между устройствами CE и PE, которая может быть указана значением согласованной (CIR[1]), избыточной (EIR[2]) или пиковой (PIR[3]) скорости. Запрошенная пропускная способность выражается как входная и выходная пропускная способность, определяемые относительно сайта абонента. Входная пропускная способность указывает скорость загрузки данных на сайт абонента, выходная - скорость выгрузки данных с сайта в сеть.

Пропускная способность настраивается только на уровне site-network-access (т. е. для соединения сайта с сетью).

Использование разных значений пропускной способности в каждом направлении позволяет SP понять возможность использования для абонента асимметричных технологий (например, ADSL). Это может применяться также для разного ограничения скорости в каждом направлении при симметричном соединении.

Параметр svc-bandwidth имеет определённый тип. Данный документ определяет 4 типа:

- bw-per-access - пропускная способность задаётся для соединения или доступа сайта в сеть применительно ко всем кадрам сервиса на интерфейсе, связанном с конкретным подключением;
- bw-per-cos - пропускная способность задаётся для класса обслуживания (CoS), определяя скорость для всех кадров данного CoS с конкретным cos-id;
- bw-per-svc - пропускная способность задаётся для сайта в целом, определяя скорость для всех кадров сервиса, связанных с конкретным экземпляром VPN;
- «непрозрачная» пропускная способность, не связанная с каким-либо cos-id, экземпляром VPN (vpn-id) или идентификатором доступа сайта в сеть.

Параметр svc-bandwidth должен включать cos-id для типа bw-per-cos. Значения cos-id могут выделяться на основе (1) значения IEEE 802.1p [IEEE-802-1D] в C-tag или (2) кода DSCP[4] в заголовке IP[5]. Измерения выполняются в соответствии с профилем пропускной способности, заданным cos-id.

Для типа bw-per-access параметр svc-bandwidth должен быть связан с конкретным параметром site-network-access-id. С каждым подключением сайта может быть связано множество значений полосы на уровне cos-id.

Для типа bw-per-svc параметр svc-bandwidth должен включать конкретный параметр vpn-id. С одним сервисом EVPN может быть связано множество значений полосы на уровне cos-id.

5.10.2. Параметр QoS

Модель определяет параметры QoS как абстракцию:

- qos-classification-policy - определяет набор упорядоченных правил классификации абонентского трафика;

[1]Committed Information Rate - согласованная скорость передачи информации.
[2]Excess Information Rate - избыточная скорость передачи информации.
[3]Peak Information Rate - пиковая скорость передачи информации.
[4]Differentiated Services Code Point - код дифференцированного обслуживания.
[5]В оригинале ошибочно сказано «в заголовке кадра Ethernet». См. http://www.rfc-editor.org/errata/eid5615. *Прим. перев.*

- qos-profile - определяет применяемый профиль планирования QoS.

5.10.2.1. Классификация QoS

Правила классификации QoS определяются параметром qos-classification-policy, который представляет собой упорядоченный список правил, которые сопоставляются с потоками или приложениями, и устанавливают подходящий целевой класс обслуживания CoS (target-class-id). Пользователь может определить сопоставление с использованием более конкретного определения потока (по MAC-адресам отправителей и получателей, cos, dscp, cos-id, color-id и т. п.). Значение color-id может быть назначено кадру для идентификации соответствия профилю QoS. Кадры сервиса считаются «зелёными» (green), если они соответствуют согласованной скорости профиля пропускной способности. «Жёлтыми» (yellow) считаются кадры, выходящие за пределы согласованной скорости, но соответствующие «избыточной» скорости профиля пропускной способности. «Красными» (red) будут кадры, выходящие за пределы согласованной и избыточной скорости в профиле пропускной способности.

При использовании определения потока пользователь может применить лист-список target-sites для указания получателя потока вместо адреса получателя. В таких случаях привязка между абстракцией сайта и применяемыми для сайта MAC-адресами должна выполняться динамически. Способы организации такой привязки выходят за рамки документа. Связь сайта с L2VPN указывается контейнером vpn-attachment. Поэтому пользователь может идентифицировать получателей в потоке целевой сети VPN с помощью листа-списка target-sites и контейнера vpn-attachment. Правила без оператора сопоставления match считаются правилами «соответствия всему» (match-all). SP может реализовать завершающее правило классификации, если абонент не задал такого правила. Используемый по умолчанию класс определяет SP. В этой модели определены некоторые приложения, но можно добавлять новые с помощью дополнений. Точное значение отождествления каждого приложения зависит от SP, поэтому провайдер должен заранее информировать абонента об использовании сопоставлений по приложениям.

5.10.2.2. Профиль QoS

Пользователь может выбрать стандартный профиль, предоставленный оператором, или создать свой профиль. Профиль QoS (qos-profile) определяет правила планирования трафика, используемые SP.

Абонентский профиль QoS определяется как список записей CoS и связанных в ними свойств, приведённых ниже.

- direction - служит для указания направления, к которому применяется qos-profile. Эта модель поддерживает направление с сайта в WAN (site-to-wan), из WAN на сайт (wan-to-site) и двухстороннее управление (bidirectional), которое применяется по умолчанию. При выборе двухстороннего управления провайдеру следует обеспечить планирование трафика в соответствии с запрошенными правилами в обоих направлениях (от SP на сайт и обратно). Например, правила планирования могут применяться на стороне PE и на стороне CE канала WAN. В направлении из WAN на сайт провайдеру следует обеспечивать планирование трафика из сети SP на сайт абонента. Например, правила управления трафиком могут быть реализованы лишь на устройстве PE, подключённом к WAN-каналу в направлении абонента.
- policing - (необязательно) указывает, следует ли применять правила к одной скорости и двум цветами или двум скоростям и трём цветам.
- byte-offset - (необязательно) указывает число байтов в заголовках кадров, которые не учитываются при ограничении скорости.
- frame-delay - ограничивает задержки для данного класса. Ограничение задержки может быть указано минимальной возможной задержкой или границей задержки в миллисекундах. Выполнение этого ограничения зависит от реализации SP - может применяться строгий механизм приоритизации для очередей на канале доступа и в ядре сети или создаваться путь маршрутизации с малой задержкой для этого класса трафика.
- frame-jitter - ограничивает вариации задержек для данного класса. Ограничение может быть выражено как минимальная возможная вариация или граница вариации в миллисекундах. Выполнение этого ограничения зависит от реализации SP - может применяться строгий механизм приоритизации для очередей на канале доступа и в ядре сети или создаваться путь маршрутизации с известной величиной вариаций для этого класса.
- bandwidth - задаёт гарантированную пропускную способность для CoS, выражаемую в процентах. Параметр guaranteed-bw-percent использует в качестве единицы отсчёта доступную пропускную способность, которой следует быть не ниже значения CIR, определённого во входном или выходном параметре svc-bandwidth. При реализации контейнера qos-profile на стороне CE в качестве единицы отсчёта применяется выходное значение svc-bandwidth, а при реализации на стороне PE - входное значение svc-bandwidth. По умолчанию резервирование пропускной способности гарантируется лишь на уровне доступа. Пользователь может применить лист end-to-end для запроса сквозного резервирования пропускной способности, включая транспортную сеть MPLS. Иными словами, SP будет активировать в ядре MPLS те или иные средства обеспечения запрошенной абонентом пропускной способности. Решение этой задачи (например, резервирование RSVP-TE или резервирование в контроллере) выходит за рамки документа.

Кроме того, условия в сети могут препятствовать выполнению провайдером некоторых ограничений. В таких случаях SP следует уведомлять абонента. Способ такого уведомления выходит за рамки документа.

5.10.3. Поддержка BUM

Контейнер broadcast-unknown-unicast-multicast указывает тип сайта в топологии групповой пересылки абонента - источник, получатель или оба сразу. Эти параметры помогают системе управления оптимизировать групповой трафик.

Можно создать множество отображений групп на порты (group-to-port) с помощью списка multicast-gp-address-mapping, определяющего адрес multicast-группы и номер порта LAG. Эти параметры помогают SP выбрать подходящую привязку интерфейса к multicast-группе для удовлетворения требований абонента.

Для обеспечения «прозрачной» доставки данного кадра все групповые кадры L2 (данные и управление) следует без изменений (за исключением VLAN ID) передавать от CE до CE. Значения VLAN ID, заданные SP, также можно менять.

Для услуг «точка-точка» провайдер должен лишь доставить одну копию каждого кадра сервиса удалённому PE, независимо от типа MAC-адреса получателя во входящем кадре (групповой, индивидуальный, широковещательный). Поэтому все кадры следует доставлять безусловно.

Пересылка кадров BUM в многоточечном сервисе включает локальную лавинную рассылку другим устройствам AC того же PE и удалённую репликацию на всех других PE, которая требует дополнительных ресурсов и пропускной способности в ядре сети. На обращённых наружу интерфейсах (UNI или E-NNI[1]) могут быть реализованы специальные правила обработки кадром BUM с ограничением скорости для них числом пакетов или битов в секунду.

Может задаваться общий порог для всего трафика BUM или отдельные пороги для каждой категории трафика.

5.11. Управление сайтом

Субконтейнер management предназначен для опций управления сайтом с учётом принадлежности устройств и контроля доступа. Ниже кратко описаны три базовые модели управления.

Управляемое провайдером устройство CE. Провайдер монопольно владеет устройством CE и только он имеет доступ к CE. Граница ответственности SP и абонента размещается между CE и сетью абонента. Этот вариант используется чаще всего.

Управляемое абонентом устройство CE. Абонент монопольно владеет устройством CE и только он имеет доступ к CE. Граница ответственности SP и абонента размещается между PE и CE.

Совместно управляемое устройство CE. Провайдер владеет устройством CE и отвечает за управление им. Однако провайдер предоставляет абоненту доступ к некоторым возможностям настройки и мониторинга CE. В этом режиме граница ответственности также размещается между CE и сетью абонента.

Выбранная модель управления указывается в листе type. Лист address хранит адрес для управления устройством CE. Лист management-transport служит для указания протокола, используемого для управления (IPv4 или IPv6). На основе выбранной модели управления могут быть заданы дополнительные опции защиты.

5.12. Защита от петель MAC

Переброс MAC-адреса между физическими портами обычно говорит о наличии петли между мостами в сети абонента. Вводящие в заблуждение записи в таблице кэширования MAC-адресов могут приводить к зацикливанию кадров сервиса в сети и перегрузке каналов через сеть провайдера, оказывающей влияние на другие услуги в этой сети. В случае EVPN это также вызывает множественные обновления BGP и нестабильность на уровне управления.

SP может реализовать механизм предотвращения петель на обращённых наружу интерфейсах для многоточечного сервиса, задав порог для переброса MAC-адресов.

Частота переброса MAC-адресов и опции предотвращения петель указываются в контейнере mac-loop-prevention.

5.13. Ограничение числа MAC-адресов

Необязательный контейнер mac-addr-limit содержит предельное число абонентских MAC-адресов и данные, описывающие поведение при достижении предела или старении MAC-адреса.

При реализации нескольких экземпляров сервиса на одном элементе сети таблица MAC-адресов (а также пространство RIB[2] для маршрутов MAC в случае EVPN) является совместно используемым ресурсом. Провайдер может ограничивать число MAC-адресов, узнанных от абонента, для одного экземпляра сервиса с помощью листа mac-addr-limit и может применять лист action для указания действий в случае превышения заданного предела - отбрасывание пакета, лавинная рассылка или просто запись события в системный журнал.

Если для услуг «точка-точка» обучение MAC отключено, ограничивать число MAC-адресов не требуется.

5.14. Расширенные возможности VPN

5.14.1. Оператор для операторов

В случае CsC[3] [RFC8299] абонент может захотеть организовать сервис MPLS на основе L2VPN для передачи трафика.

В примере на рисунке 21 ISP1 продаёт услуги L2VPN, но не имеет инфраструктуры ядра между своими точками POP и использует сервис L2VPN в качестве такой инфраструктуры (принадлежащей другому провайдеру) между своими POP.

[1]External NNI - внешний интерфейс между сетями.
[2]Routing Information Base - база маршрутной информации.
[3]Carriers' Carriers - оператор для операторов.

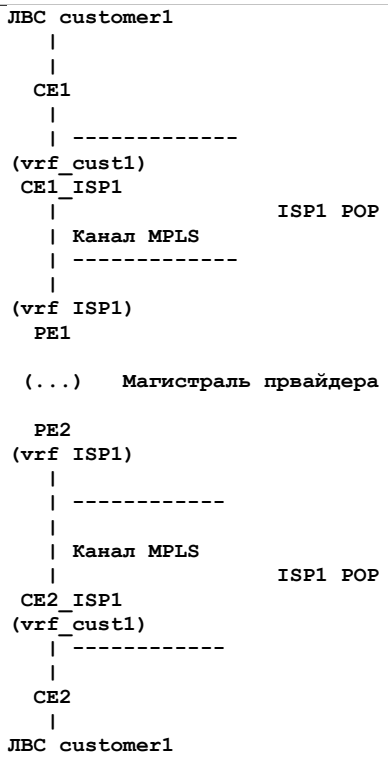

Рисунок 21. Сервис MPLS с использованием L2VPN.

Для поддержки CsC сервис VPN должен указать поддержку MPLS путём указания для листа carrierscarrier в списке vpn-service значения true. Канал между CE1_ISP1/PE1 и CE2_ISP1/PE2 должен также поддерживать протокол сигнализации MPLS. Конфигурация выполняется на уровне сайта.

В этой модели в качестве сигнального протокола MPLS может применяться LDP или BGP. В случае LDP **должен** также применяться протокол внутренней маршрутизации IGP. В случае сигнализации BGP протокол BGP **должен** также служить протоколом маршрутизации.

При использовании CsC запрашиваемый лист svc-mtu должен указывать MPLS MTU, а не MTU на канале.

5.15. Ссылки на внешние идентификаторы

Модель сервиса порой обращается к внешней информации путём задания идентификаторов. Например, для заказа доступа в облако конкретного CSP[1] в модели используется идентификатор целевого CSP. Если абонент напрямую применяет модель сервиса в качестве API (например, через RESTCONF или NETCONF) для заказа определённой услуги, провайдеру следует предоставлять список действующих идентификаторов. В случае доступа к облаку SP будет предоставлять идентификаторы, связанные с доступными провайдерами CSP. То же самое относится и к другим идентификаторам (таким, как qos-profile).

Например, установка remote-carrier-name используется в случае NNI, поскольку эта информация нужна текущему L2VPN SP, с которым организуется соединение, тогда как идентификатор облака (cloud-identifier) нужен текущему L2VPN SP и абоненту, поскольку он применяется для доступа к публичному облаку или в Internet.

Способы предоставления провайдером этой информации абоненту выходят за рамки документа.

5.16. Определение NNI и поддержка нескольких AS

Автономная система (AS[2]) представляет собой сеть или группу сетей с единым администрированием, которая использует один чётко определённый протокол маршрутизации. В некоторых случаях требуется организовать VPN через несколько AS, разделённых географически или относящихся к разным SP. Соединения между AS организуются провайдерами и не видны абоненту. Примеры таких соединений включают:

- партнерские отношения между SP (например, оператор или облако) для расширения сервиса VPN;
- внутренние границы в рамках одного SP (например, транзитные сети, ядро и ЦОД).

Интерфейсы NNI определяются для организации VPN через множество AS. В [RFC4761] определено множество вариантов реализации VPN NNI (например, VPLS), каждый из которых имеет свои преимущества и недостатки, но этот вопрос выходит за рамки документа. Например в варианте A (две AS) партнёры ASBR[3] соединяются через множество интерфейсов, из которых по крайнем мере один, относящийся в обеим AS, будет присутствовать в VPN. Чтобы эти ASBR могли обмениваться блоками меток, они связывают каждый интерфейс с таблицей MAC-VRF (VSI, раздел 2) и сессией BGP. В результате трафик между устройствами в VPLS передаётся по протоколу Ethernet. В этом варианте все VPN изолированы одна от другой, а поскольку трафик передаются с помощью Ethernet, механизмы QoS для трафика Ethernet могут применяться для обеспечения абонентских соглашений SLA.

На рисунке 22 показана сеть SP (Моя сеть), имеющая несколько интерфейсов NNI, используемых для

[1]Cloud Service Provider - поставщик облачных услуг.
[2]Autonomous System.
[3]AS Border Router - граничный маршрутизатор AS.

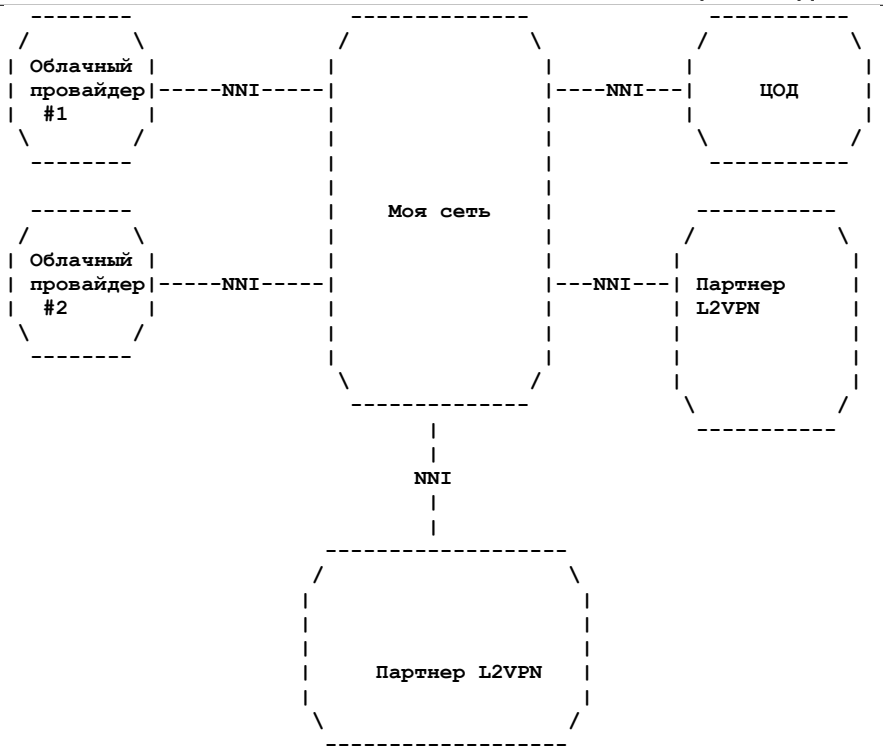

Рисунок 22. Сеть SP с несколькими NNI.

- расширения своего присутствия, основанного на партнёрстве L2VPN;
- подключения своих ЦОД к абонентским L2VPN;
- обеспечения абонентам доступа к частным ресурсам, расположенным в облаке некого провайдера CSP.

5.16.1. Определение NNI, вариант A

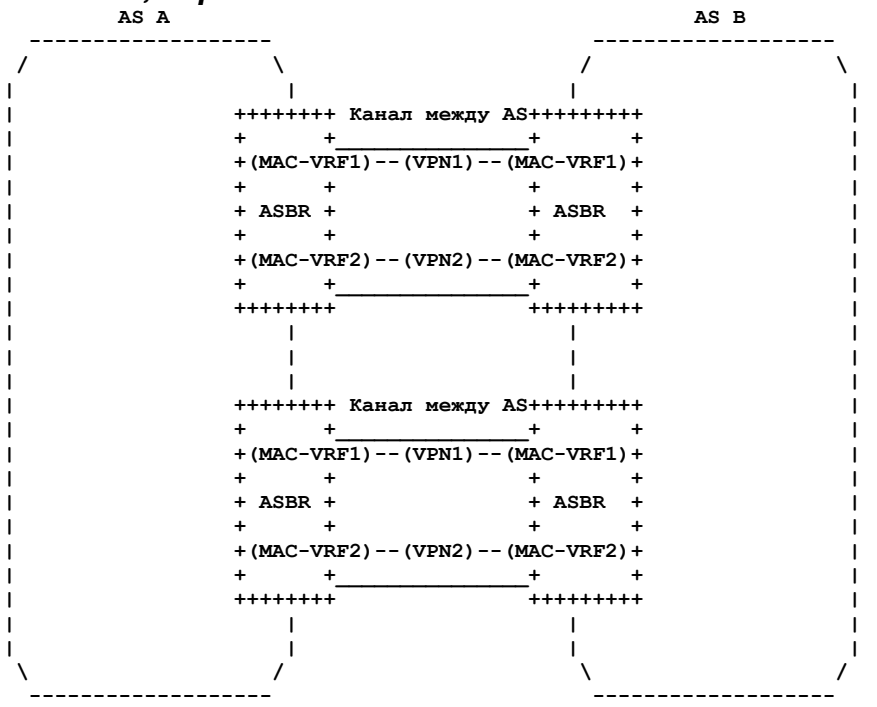

Рисунок 23. Интерфейс NNI, вариант A, пример 1.

В варианте A две AS соединены между собой физическими каналами на маршрутизаторах ASBR. Для отказоустойчивости между AS может быть организовано множество физических соединений. Соединение VPN (физическое или логическое на основе физического) создаётся для каждой сети VPN, которой требуется выход за границу AS.

С точки зрения модели сервиса это соединение VPN может выглядеть сайтом. Предположим, что AS B хочет расширить соединение для VPN C на AS A. Администратор AS B может использовать эту модель сервиса для заказа сайта в AS A. Все варианты могут быть реализованы с использованием возможностей текущей модели. Например, на рисунке 23 показаны два физических соединения, на которые наложены логические соединения VPN. Это можно рассматривать как сценарий с множеством VPN. Администратор AS B может также выбрать подходящий протокол маршрутизации (например, EBGP[1]) для динамического обмена маршрутами между AS.

[1]External BGP - внешний BGP.

В этом документе предполагается, что для варианта A интерфейса NNI **следует** применять имеющуюся модель сайта VPN.

На рисунке 24 показан пример, где абонент хочет, чтобы его CSP A присоединил свою виртуальную сеть N к имеющейся L2VPN (VPN1) от сервиса L2VPN провайдера SP B.

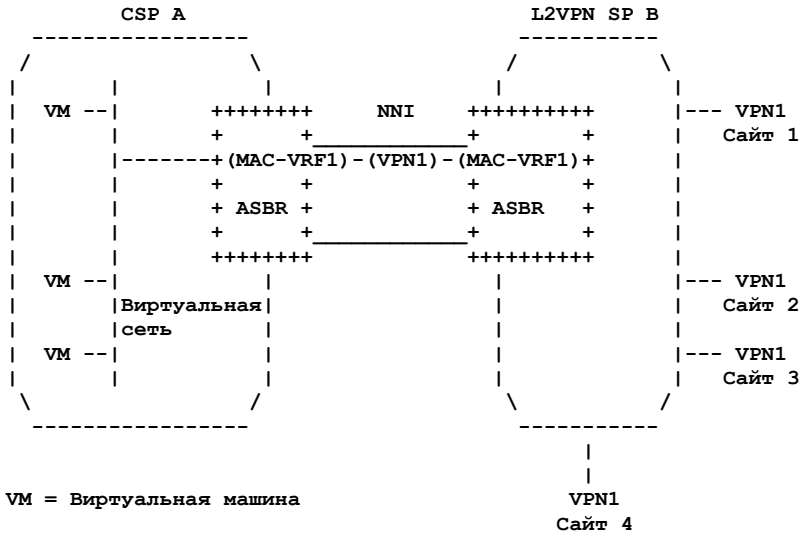

Рисунок 24. Интерфейс NNI, вариант A, пример 2.

Для подключения VPN провайдер CSP или абонент может использовать модель L2SM, раскрытую провайдером SP B. Поскольку интерфейс NNI используется совместно, можно считать, что физическое соединение (bearer) между CSP A и SP B уже имеется. CSP A может запросить через модель сервиса создание нового сайта с одним контейнером site-network-access (single-homing на рисунке 24). В качестве ограничения для размещения CSP A может использовать ссылку на носитель (bearer) от SP A для размещения VPN NNI на имеющемся канале. Приведённый ниже код XML иллюстрирует возможный запрос конфигурации к провайдеру SP B.

```
<?xml version="1.0"?>
<l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
 <vpn-profiles>
  <valid-provider-identifiers>
   <qos-profile-identifier>
    <id>GOLD</id>
   </qos-profile-identifier>
   <qos-profile-identifier>
    <id>PLATINUM</id>
   </qos-profile-identifier>
  </valid-provider-identifiers>
 </vpn-profiles>
 <vpn-services>
  <vpn-service>
   <vpn-id>VPN1</vpn-id>
   <ce-vlan-preservation>true</ce-vlan-preservation>
   <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
  </vpn-service>
 </vpn-services>
 <sites>
      <site>
          <site-id>CSP_A_attachment</site-id>
           <locations>
            <location>
              <location-id>NY1</location-id>
              <city>NY</city>
              <country-code>US</country-code>
           </location>
           </locations>
          <site-vpn-flavor>site-vpn-flavor-nni</site-vpn-flavor>
            <site-network-accesses>
              <site-network-access>
               <network-access-id>CSP_A_VN1</network-access-id>
                       <connection>
                       <encapsulation-type>vlan</encapsulation-type>
                       <eth-inf-type>tagged</eth-inf-type>
                        <tagged-interface>
                         <tagged-inf-type>dot1q</tagged-inf-type>
                         <dot1q-vlan-tagged>
                          <cvlan-id>17</cvlan-id>
                        </dot1q-vlan-tagged>
                        </tagged-interface>
                       </connection>
                         <service>
                           <svc-bandwidth>
                             <bandwidth>
                              <direction>input-bw</direction>
                               <type>bw-per-cos</type>
                                <cir>450000000</cir>
```

```
                                <cbs>20000000</cbs>
                                <eir>1000000000</eir>
                                <ebs>200000000</ebs>
                              </bandwidth>
                            </svc-bandwidth>
                            <carrierscarrier>
                              <signaling-type>bgp</signaling-type>
                             </carrierscarrier>
                           </service>
                          <vpn-attachment>
                            <vpn-id>12456487</vpn-id>
                            <site-role>spoke-role</site-role>
                           </vpn-attachment>
                    </site-network-access>
                </site-network-accesses>
                <management>
                 <type>customer-managed</type>
                </management>
            </site>
     </sites>
    </l2vpn-svc>
```

Описанный выше случай отличается от сценария использования контейнера cloud-accesses, который обеспечивает доступ в публичное облако, тогда как в примере организуется доступ к приватным ресурсам в сети CSP.

5.16.2. Определение NNI, вариант B

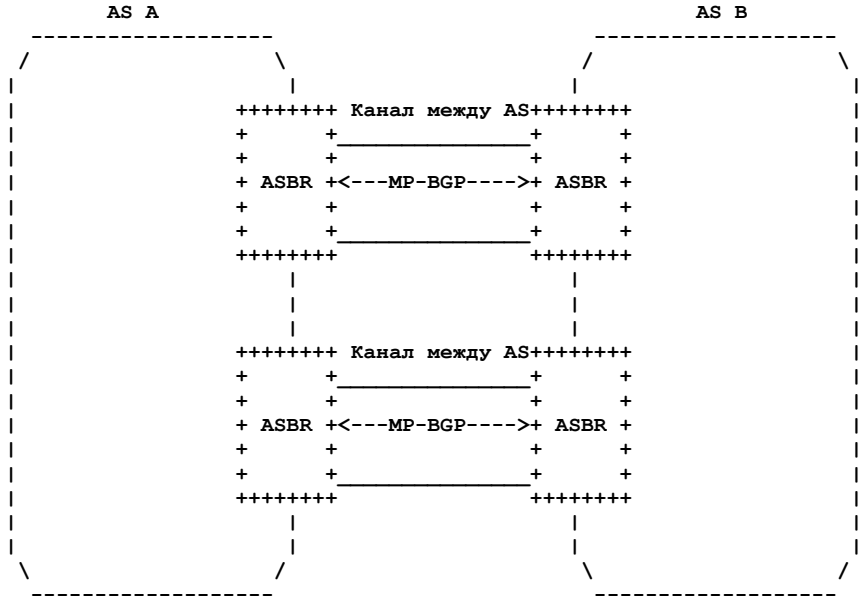

Рисунок 25. Интерфейс NNI, вариант B, пример 1.

В варианте B две AS соединены между собой физическими каналами на ASBR. Для отказоустойчивости может использоваться множество соединений между AS. «VPN-соединение» между AS организуется путём обмена маршрутами VPN с использованием MP-BGP [RFC4761].

Существует три варианта реализации такого интерфейса NNI.

1. NNI является внутренним для провайдера и расположен между магистралью и ЦОД. Домены являются доверенными и не нужно фильтровать маршруты VPN, т. е. обмен происходит для всех маршрутов. Может применяться фильтрация RT для сохранения некоторых необязательных состояний.
2. NNI располагается между провайдерами, готовыми обмениваться маршрутами VPN лишь для конкретных RT. Каждый провайдер получил от другого полномочия на использование этих значений RT.
3. NNI располагается между провайдерами, готовыми обмениваться маршрутами VPN лишь для конкретных RT. Каждый провайдер имеет свою схему RT. Поэтому работающие через две сети абоненты будут получать для конкретной VPN разные RT в каждой сети.

В случае 1 модель сервиса не нужна, поскольку протокол позволяет динамический обмен нужными маршрутами VPN.

В случае 2 требуется политика фильтрации RT на ASBR. С точки зрения модели сервиса требуется согласовать список RT для передачи полномочий.

В случае 3 обе AS должны согласовать VPN RT для обмена, а также отображение VPN RT одной AS на RT из другой.

Такое моделирование выходит за рамки этого документа.

На рисунке 26 показано соединение NNI между CSP A и сетью SP B. Провайдеры не доверяют друг другу и каждый применяет свои правила выделения RT. Поэтому в терминах реализации абонентская VPN имеет своё значение RT в каждой сети (RT A в CSP A и RT B в сети SP B). Для подключения виртуальной сети абонента в CSP A к абонентской L2VPN (VPN1) в сети SP B провайдеру CSP A следует запросить у сети SP B создание абонентской VPN на интерфейсе NNI (восприятие соответствующего RT). Трансляция RT выполняется на основе соглашения между двумя SP - SP B может разрешить CSP A запрос трансляции VPN (RT).

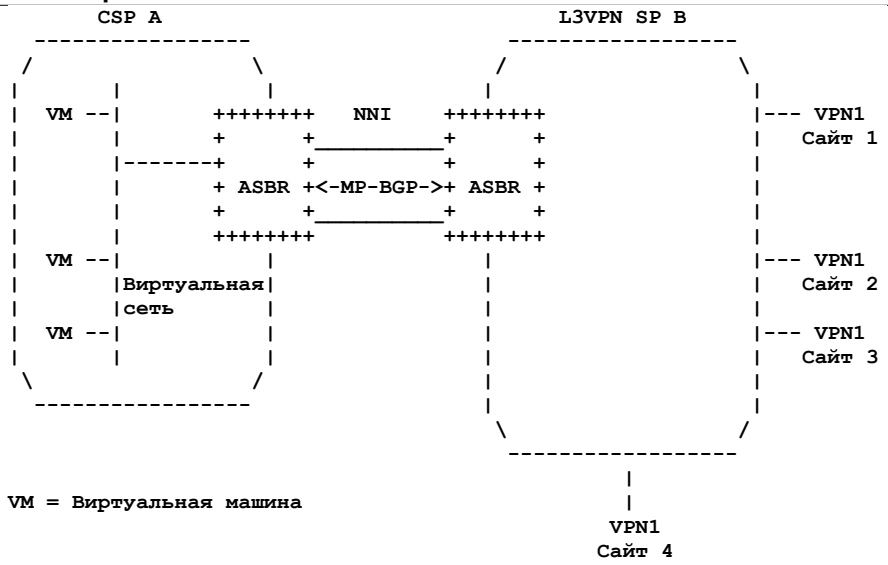

Рисунок 26. Интерфейс NNI, вариант B, пример 2.

5.16.3. Определение NNI, вариант C

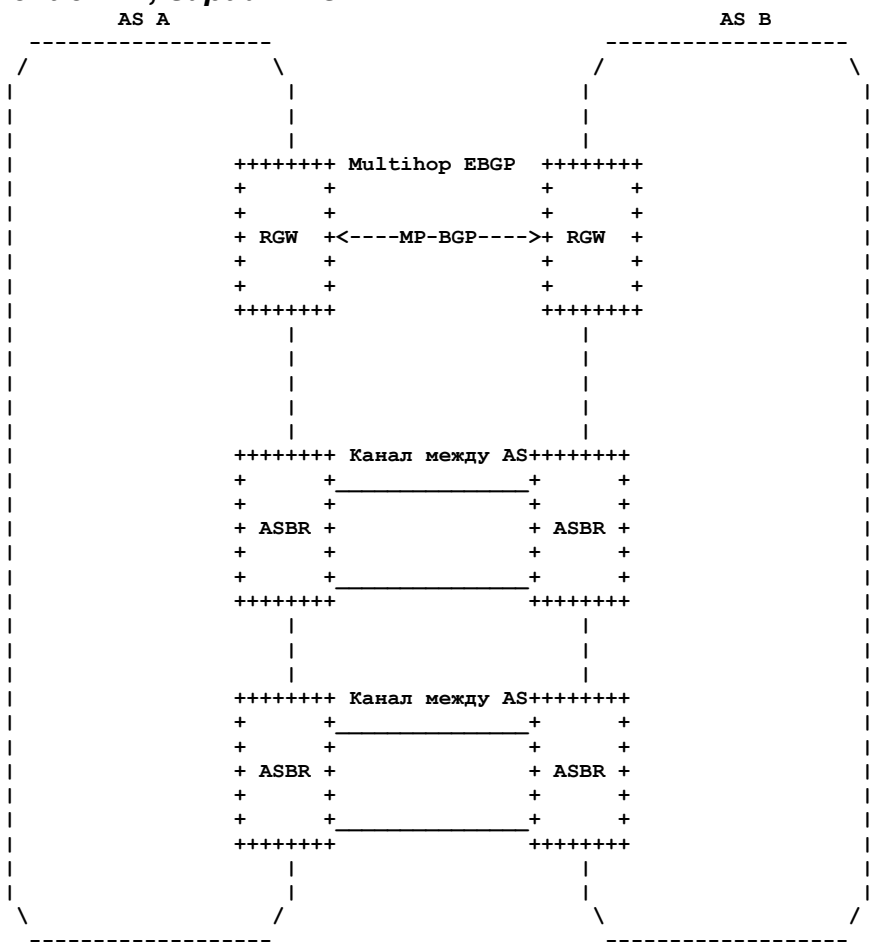

Рисунок 27. Вариант C для NNI.

С точки зрения сервиса VPN вариант C для NNI очень похож на вариант B, поскольку используется сессия MP-BGP для обмена маршрутами VPN между AS. Различие состоит в том, что уровни пересылки и управления размещаются на разных узлах, поскольку сессия MP-BGP включает несколько этапов пересылки между шлюзами маршрутизации (RGW). С точки зрения сервиса VPN моделирование вариантов B и C выполняется идентично.

5.17. Применимость L2SM в межпровайдерской и междоменной оркестровке

В случаях, когда AS относятся к разным провайдерам, можно предположить заинтересованность провайдеров в снижении числа сигнальных сессий через границу AS и ограничении набора устройств, на которых завершаются такие сессии. Здесь возможны два подхода:

(a) создание межпровайдерских управляющих соединений, которые работают лишь между двумя граничными маршрутизаторами;

(b) разрешение организовывать сквозные многосегментные соединения без поддержки сквозного управляющего соединения.

Межпровайдерские управляющие соединения варианта (a) могут быть реализованы с использованием методов, описанных в параграфе 5.16 (например, определение NNI). Многосегментные соединения варианта (b) могут приводить

к решениям для соединений между AS, похожим на схему (b) в разделе 10 [RFC4364]. Это можно реализовать путём «сшивания» соединений сайтов и сегментов сервиса в разных доменах. Например, сквозное соединение между сайтами 1 и 3 через множество доменов (скажем, городские сети) может быть организовано путём сшивания соединений доступа на сайте 1 с SEG1, SEG3, SEG4, а также с подключением к сети на сайте 3 (как показано на рисунке 28). Предполагается, что компонент оркестровки на рисунке 3 должен иметь представление о полной абстрактной топологии и доступности ресурсов. Это может основываться на планировании сети.

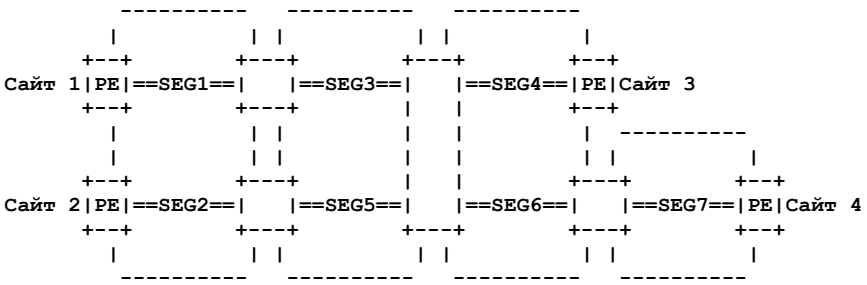

Рисунок 28. Пример межпровайдерской и междоменной оркестровки.

Отметим, что SEG1, SEG2, SEG3, SEG4, SEG5 и SEG6 можно рассматривать как подключения доступа на сайте и они могут быть созданы как подключения обычных сайтов с использованием L2SM.

На рисунке 28 протокол BGP служит для распространения L2VPN NLRI[1] из одной AS в соседнюю. Сначала маршрутизаторы PE используют BGP для распространения L2VPN NLRI маршрутизаторам ASBR или рефлекторам маршрутов, клиентами которых являются ASBR. Затем ASBR использует BGP для распространения этих L2VPN NLRI маршрутизатору ASBR в другой AS, который далее распространит их маршрутизаторам PE в своей AS или, возможно, другим ASBR, которые разошлют анонсы дальше.

В этом случае PE может узнать адрес маршрутизатора ASBR, через который доступен другой PE, для организации соединения с последним. Т. е. локальный PE будет получать анонс BGP с L2VPN NLRI для экземпляра L2VPN, где у локального PE есть подключённые участники. Следующим интервалом BGP в этом L2VPN NLRI будет ASBR локальной AS. Затем вместо создания управляющего соединения через весь путь с удаленным PE, локальный PE создаст соединение лишь с ASBR, т. е. сегмент соединения от PE до ASBR. Маршрутизатор ASBR может организовать соединение с ASBR в следующей AS, а затем «сшить» с соединением от PE, как описано в [RFC6073]. Повторение процедуры на каждом ASBR создаст цепочку соединений, которая после «сшивания» свяжет два маршрутизатора PE.

Отметим, что при описанном подходе локальный маршрутизатор PE может никогда не узнать IP-адрес удалённого PE. Он знает L2VPN NLRI из анонсов удалённого PE, который не обязан включать адрес удалённого PE, и знает IP-адрес ASBR, который служит следующим интервалом BGP для данного NLRI.

При использовании такого подхода для VPLS или полносвязной (full-mesh) VPWS возникает полносвязный набор соединений между PE, но полносвязные управляющие соединения (сессии LDP или L2TPv3) не требуются. Вместо этого управляющие соединения внутри AS организуются между всеми PE данной AS и маршрутизаторами ASBR этой AS. Одно управляющее соединение между ASBR смежных AS может поддерживать множество сегментов соединений AS-AS, если они нужны.

6. Взаимодействие с другими модулями YANG

Как разъяснено в разделе 4, эта модель сервиса не предназначена для элементов сети, а реализуется в системе управления.

Система управления может иметь модульную конструкцию и включать две разных части:

a. компонент, отвечающий за модель сервиса (назовём его сервисным компонентом);

b. компонент, отвечающий за настройку элементов сети (назовём его конфигурационным компонентом).

В некоторых случаях, когда требуется отделить поведение и запрашиваемые абонентом функции от сетевой технологии, которую оператор использует для предоставления услуги [RFC8309], из сервисного компонента может быть выделен новый компонент (назовём его управляющим). Этот компонент отвечает за работу сети и осведомлен о многих свойствах, включая топологию, технологию и политику оператора. Будучи необязательным, этот компонент может использовать модель сервиса в качестве входной информации. Этот компонент может передать все полномочия управления конфигурационному компоненту.

В разделе 7 приведён пример трансляции запросов на предоставление сервиса в строки конфигурации маршрутизатора. В экосистеме на основе YANG предполагается использование NETCONF и YANG между конфигурационным компонентом и сетевыми элементами для настройки запрошенного сервиса на этих элементах.

В этой схеме предполагается, что модели данных YANG будут применяться для настройки компонент сервиса на элементах сети. Будет существовать тесная связь между абстрактным представлением, обеспечиваемым этой моделью сервиса, и детальным представлением конфигурации, которое будет обеспечиваться конкретными моделями конфигурации для элементов сети, такими как определены в [MPLS-L2VPN-YANG] и [EVPN-YANG]. Компоненты сервиса, для которых нужна настройка элементов сети для поддержки определённой здесь модели сервиса, включают:

- определения экземпляров сетей, которые включают правила VPN;
- физические интерфейсы;
- параметры уровня Ethernet (например, идентификаторы VLAN);
- QoS (классификация, профили и т. п.);

[1]Network Layer Reachability Information - информация о доступности на сетевом уровне.

- поддержка Ethernet Service OAM.

7. Пример использования модели сервиса

Как разъяснено в разделе 4, эта модель сервиса предназначена для реализации на уровне управления и не рассчитана на прямое использование элементами сети. Система управления служит центральной точкой настройки сервиса в целом.

В этом разделе приведён пример использования модели системой управления для настройки сервиса L2VPN на элементах сети.

В приведённом ниже примере сервис VPN организуется для 3 сайтов, использующих VPWS «точка-точка» и топологию сервиса VPN Hub-and-Spoke, как показано на рисунке 29. Распределение нагрузки здесь не рассматривается.

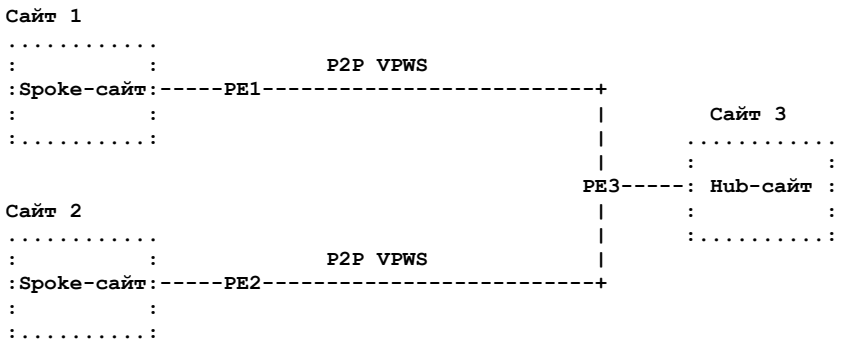

Рисунок 29. Эталонная сеть для простого примера.

Приведённый ниже код XML упрощенно описывает общую конфигурацию сервиса для этой сети VPN.

```
<?xml version="1.0"?>
<l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
  <vpn-services>
      <vpn-service>
       <vpn-id>12456487</vpn-id>
        <vpn-svc-type>vpws</vpn-svc-type>
        <svc-topo>hub-spoke</svc-topo>
        <ce-vlan-preservation>true</ce-vlan-preservation>
        <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
       </vpn-service>
      <vpn-service>
        <vpn-id>12456488</vpn-id>
        <vpn-svc-type>vpws</vpn-svc-type>
        <svc-topo>hub-spoke</svc-topo>
        <ce-vlan-preservation>true</ce-vlan-preservation>
        <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
       </vpn-service>
  </vpn-services>
</l2vpn-svc>
```

При получении запроса на организацию сервиса VPN система управления будет внутренними средствами (или путём взаимодействия с другими компонентами OSS) выделять значения VPN RT. В данном конкретном случае будут выделены два значения RT (100:1 для концентраторов и 100:2 для лучей). Приведённый ниже результат описывает конфигурацию Spoke-сайта 1.

```
<?xml version="1.0"?>
<l2vpn-svc xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc">
 <vpn-services>
  <vpn-service>
   <vpn-id>12456487</vpn-id>
   <svc-topo>hub-spoke</svc-topo>
   <ce-vlan-preservation>true</ce-vlan-preservation>
   <ce-vlan-cos-preservation>true</ce-vlan-cos-preservation>
  </vpn-service>
 </vpn-services>
 <sites>
   <site>
      <site-id>Spoke_Site1</site-id>
         <locations>
           <location>
            <location-id>NY1</location-id>
            <city>NY</city>
            <country-code>US</country-code>
           </location>
          </locations>
          <site-network-accesses>
             <site-network-access>
                <network-access-id>Spoke_UNI-Site1</network-access-id>
                  <access-diversity>
                    <groups>
                      <group>
                        <group-id>20</group-id>
                      </group>
                    </groups>
                  </access-diversity>
```

```
                    <connection>
                     <encapsulation-type>vlan</encapsulation-type>
                      <tagged-interface>
                      <dot1q-vlan-tagged>
                        <cvlan-id>17</cvlan-id>
                      </dot1q-vlan-tagged>
                      </tagged-interface>
                      <l2cp-control>
                        <stp-rstp-mstp>tunnel</stp-rstp-mstp>
                        <lldp>true</lldp>
                      </l2cp-control>
                    </connection>
                    <service>
                      <svc-bandwidth>
                        <bandwidth>
                         <direction>input-bw</direction>
                          <type>bw-per-cos</type>
                           <cir>450000000</cir>
                           <cbs>20000000</cbs>
                           <eir>1000000000</eir>
                           <ebs>200000000</ebs>
                        </bandwidth>
                      </svc-bandwidth>
                      <carrierscarrier>
                       <signaling-type>bgp</signaling-type>
                      </carrierscarrier>
                    </service>
                     <vpn-attachment>
                       <vpn-id>12456487</vpn-id>
                       <site-role>spoke-role</site-role>
                     </vpn-attachment>
                   </site-network-access>
                 </site-network-accesses>
                 <management>
                   <type>provider-managed</type>
                 </management>
               </site>
         </sites>
      </l2vpn-svc>
```

При получении запроса на предоставление Spoke-сайта 1 система управления **должна** выделить сетевые ресурсы для этого сайта. Она **должна** сначала определить целевые элементы сети для предоставления доступа и, в частности, устройство PE (возможно, агрегирующий коммутатор). Как описано в параграфах 5.3.1 и 5.6, системе управления **следует** использовать данные о местоположении и она **должна** применять ограничения при доступе (access-diversity) для поиска подходящего PE. В этом случае мы считаем, что Spoke-сайт 1 требует разнесения PE с Hub-сайтами и система управления будет выбирать PE по наименьшей удалённости. На основе данных о местоположении система управления найдёт доступные PE в ближней к абоненту окрестности и укажет среди них подходящий по требованиям к разнесению доступа.

После выбора PE система управления должна выделить интерфейсные ресурсы на узле. Из доступных ресурсов PE выбирается один интерфейс. Система управления может начать инициализацию узла PE, используя любые удобные средства (например, NETCONF, CLI). Система управления проверит наличие таблицы виртуальной маршрутизации VSI, соответствующей потребностям. Если такой таблицы нет, система предоставит её - значение RD будет выбрано в соответствии с внутренней политикой, а значения RT будут выведены из конфигурации vpn-policy для сайта (т. е. система управления будет выделять некие значения RT для VPN). Поскольку сайт относится к типу Spoke (site-role), система управления знает, какие RT должны экспортироваться и импортироваться. Сайт управляется провайдером, поэтому могут быть добавлены значения RT для управления (100:5000). В конфигурацию **могут** также добавляться стандартные для провайдера правила VPN.

Пример созданной конфигурации PE приведён ниже.

```
l2vpn vsi context one
  vpn id 12456487
     autodiscovery bgp signaling bgp
     ve id 1001     <---- Указывает маршрутизаторы PE в домене VPLS
     ve range 50    <---- Размер VPLS Edge (VE)
     route-distinguisher 100:3123234324
     route-target import 100:1
     route-target import 100:5000    <---- Стандартная конфигурация SP
     route-target export 100:2             для управляемого провайдером CE
   !
```

Когда таблица VSI предоставлена, система управления может начать настройку доступа на PE с использованием информации о выделенном интерфейсе. Тег или VLAN (например, тег экземпляра сервиса) выбирается системой управления. Один тег будет выбран из выделенной для PE подсети, другой будет служить для настройки CE.

Между PE и CE будут также настроены протоколы LACP. В модели с провайдерским управлением это будет делать SP. Этот выбор не зависит от протокола LACP, выбранного абонентом.

Пример созданной конфигурации PE показан ниже.

```
   !
   bridge-domain 1
    member Ethernet0/0 service-instance 100
    member vsi one
   !
   l2 router-id 198.51.100.1
   !
   l2 router-id 2001:db8::10:1/64
   !

   interface Ethernet0/0
    no ip address
    service instance 100 ethernet
   encapsulation dot1q 100
    !

   !
   router bgp 1
    bgp log-neighbor-changes
    neighbor 198.51.100.4 remote-as 1
    neighbor 198.51.100.4 update-source Loopback0
    !
    address-family l2vpn vpls
     neighbor 198.51.100.4 activate
     neighbor 198.51.100.4 send-community extended
     neighbor 198.51.100.4 suppress-signaling-protocol ldp
     neighbor 2001:db8::0a10:4 activate
     neighbor 2001:db8::0a10:4 send-community extended
    exit-address-family

   !
   interface vlan 100     <---- Связывание AC с MAC-VRF на PE
     no ip address
     xconnect vsi PE1-VPLS-A
   !
   vlan 100
     state active
```

Поскольку маршрутизатор CE на этом этапе не доступен, система управления может создать полную конфигурацию CE для загрузки вручную (например, до передачи устройства CE абоненту, как описано в параграфе 5.3.1). Конфигурация CE будет создаваться таким же способом, как для устройства PE. На основе (1) типа CE (производитель, модель), выделенного абоненту, и (2) данных о носителе (bearer) система управления определяет требующий настройки интерфейс CE. Предполагается, что настройка канала PE-CE будет выполняться автоматически с использованием провайдерской системы OSS, поскольку оба ресурса обслуживаются внутри. Параметры интерфейса между CE и ЛВС, такие как теги dot1Q, выводятся из соединения Ethernet с учётом распространения системой управления тегов dot1Q между PE и CE внутри подсети. Это позволяет создать для CE конфигурацию plug'n'play.

Пример созданной конфигурации CE показан ниже.

```
   interface Ethernet0/1
     switchport trunk allowed vlan none
     switchport mode trunk
     service instance 100 ethernet
     encapsulation default
     l2protocol forward cdp
     xconnect 203.0.113.1 100 encapsulation mpls
   !
```

8. Модуль YANG

Этот модуль YANG импортирует определения типов (typedef) из [RFC6991] и [RFC8341].

```
<CODE BEGINS> file "ietf-l2vpn-svc@2018-10-09.yang"
module ietf-l2vpn-svc {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc";
  prefix l2vpn-svc;

  import ietf-inet-types {
    prefix inet;
  }
  import ietf-yang-types {
    prefix yang;
  }
  import ietf-netconf-acm {
    prefix nacm;
  }

  organization
    "IETF L2SM Working Group.";
  contact
    "WG Web:   <https://datatracker.ietf.org/wg/l2sm/>
     WG List:  <mailto:l2sm@ietf.org>
     Editor:   Giuseppe Fioccola
               <mailto:giuseppe.fioccola@tim.it>";
  description
    "This YANG module defines a generic service configuration model
```

```
    for Layer 2 VPN services common across all vendor
    implementations.

    Copyright (c) 2018 IETF Trust and the persons
    identified as authors of the code.  All rights reserved.

    Redistribution and use in source and binary forms, with or
    without modification, is permitted pursuant to, and subject
    to the license terms contained in, the Simplified BSD License
    set forth in Section 4.c of the IETF Trust's Legal Provisions
    Relating to IETF Documents
    (https://trustee.ietf.org/license-info).

    This version of this YANG module is part of RFC 8466;
    see the RFC itself for full legal notices.";

  revision 2018-10-09 {
    description
      "Initial revision.";
    reference
      "RFC 8466: A YANG Data Model for Layer 2 Virtual Private
       Network (L2VPN) Service Delivery";
  }

  feature carrierscarrier {
    description
      "Enables the support of carriers' carriers (CsC).";
  }

  feature ethernet-oam {
    description
      "Enables the support of Ethernet Service OAM.";
  }

  feature extranet-vpn {
    description
      "Enables the support of extranet VPNs.";
  }

  feature l2cp-control {
    description
      "Enables the support of L2CP control.";
  }

  feature input-bw {
    description
      "Enables the support of input bandwidth in a VPN.";
  }

  feature output-bw {
    description
      "Enables the support of output bandwidth in a VPN.";
  }

  feature uni-list {
    description
      "Enables the support of a list of UNIs in a VPN.";
  }

  feature cloud-access {
    description
      "Allows the VPN to connect to a Cloud Service Provider (CSP)
       or an ISP.";
  }

  feature oam-3ah {
    description
      "Enables the support of OAM 802.3ah.";
  }

  feature micro-bfd {
    description
      "Enables the support of micro-BFD.";
  }

  feature bfd {
    description
      "Enables the support of BFD.";
  }

  feature signaling-options {
    description
      "Enables the support of signaling options.";
  }

  feature site-diversity {
```

```
    description
      "Enables the support of site diversity constraints in a VPN.";
  }

  feature encryption {
    description
      "Enables the support of encryption.";
  }

  feature always-on {
    description
      "Enables support for the 'always-on' access constraint.";
  }

  feature requested-type {
    description
      "Enables support for the 'requested-type' access constraint.";
  }

  feature bearer-reference {
    description
      "Enables support for the 'bearer-reference' access
       constraint.";
  }

  feature qos {
    description
      "Enables support for QoS.";
  }

  feature qos-custom {
    description
      "Enables the support of a custom QoS profile.";
  }

  feature lag-interface {
    description
      "Enables LAG interfaces.";
  }

  feature vlan {
    description
      "Enables the support of VLANs.";
  }

  feature dot1q {
    description
      "Enables the support of dot1Q.";
  }

  feature qinq {
    description
      "Enables the support of QinQ.";
  }

  feature qinany {
    description
      "Enables the support of QinAny.";
  }

  feature vxlan {
    description
      "Enables the support of VXLANs.";
  }

  feature lan-tag {
    description
      "Enables LAN tag support in a VPN.";
  }

  feature target-sites {
    description
      "Enables the support of the 'target-sites'
       match-flow parameter.";
  }

  feature bum {
    description
      "Enables BUM capabilities in a VPN.";
  }

  feature mac-loop-prevention {
    description
      "Enables the MAC loop-prevention capability in a VPN.";
  }
```

```
  feature lacp {
    description
      "Enables the Link Aggregation Control Protocol (LACP)
       capability in a VPN.";
  }

  feature mac-addr-limit {
    description
      "Enables the MAC address limit capability in a VPN.";
  }

  feature acl {
    description
      "Enables the ACL capability in a VPN.";
  }

  feature cfm {
    description
      "Enables the 802.1ag CFM capability in a VPN.";
  }

  feature y-1731 {
    description
      "Enables the Y.1731 capability in a VPN.";
  }

  typedef svc-id {
    type string;
    description
      "Defines the type of service component identifier.";
  }

  typedef ccm-priority-type {
    type uint8 {
      range "0..7";
    }
    description
      "A 3-bit priority value to be used in the VLAN tag,
       if present in the transmitted frame.";
  }

  typedef control-mode {
    type enumeration {
      enum peer {
        description
          "'peer' mode, i.e., participate in the protocol towards
           the CE.  Peering is common for LACP and the Ethernet
           Local Management Interface (E-LMI) and, occasionally,
           for LLDP.  For VPLSs and VPWSs, the subscriber can also
           request that the SP peer enable spanning tree.";
      }
      enum tunnel {
        description
          "'tunnel' mode, i.e., pass to the egress or destination
           site.  For EPLs, the expectation is that L2CP frames are
           tunneled.";
      }
      enum discard {
        description
          "'discard' mode, i.e., discard the frame.";
      }
    }
    description
      "Defines the type of control mode on L2CP protocols.";
  }

  typedef neg-mode {
    type enumeration {
      enum full-duplex {
        description
          "Defines full-duplex mode.";
      }
      enum auto-neg {
        description
          "Defines auto-negotiation mode.";
      }
    }
    description
      "Defines the type of negotiation mode.";
  }

  identity site-network-access-type {
    description
      "Base identity for the site-network-access type.";
  }
```

```
  identity point-to-point {
    base site-network-access-type;
    description
      "Identity for a point-to-point connection.";
  }

  identity multipoint {
    base site-network-access-type;
    description
      "Identity for a multipoint connection, e.g.,
       an Ethernet broadcast segment.";
  }

  identity tag-type {
    description
      "Base identity from which all tag types are derived.";
  }

  identity c-vlan {
    base tag-type;
    description
      "A CVLAN tag, normally using the 0x8100 Ethertype.";
  }

  identity s-vlan {
    base tag-type;
    description
      "An SVLAN tag.";
  }

  identity c-s-vlan {
    base tag-type;
    description
      "Using both a CVLAN tag and an SVLAN tag.";
  }

  identity multicast-tree-type {
    description
      "Base identity for the multicast tree type.";
  }

  identity ssm-tree-type {
    base multicast-tree-type;
    description
      "Identity for the Source-Specific Multicast (SSM) tree type.";
    reference "RFC 8299: YANG Data Model for L3VPN Service Delivery";
  }

  identity asm-tree-type {
    base multicast-tree-type;
    description
      "Identity for the Any-Source Multicast (ASM) tree type.";
    reference "RFC 8299: YANG Data Model for L3VPN Service Delivery";
  }

  identity bidir-tree-type {
    base multicast-tree-type;
    description
      "Identity for the bidirectional tree type.";
    reference "RFC 8299: YANG Data Model for L3VPN Service Delivery";
  }

  identity multicast-gp-address-mapping {
    description
      "Identity for mapping type.";
  }

  identity static-mapping {
    base multicast-gp-address-mapping;
    description
      "Identity for static mapping, i.e., attach the interface
       to the multicast group as a static member.";
  }

  identity dynamic-mapping {
    base multicast-gp-address-mapping;
    description
      "Identity for dynamic mapping, i.e., an interface was added
       to the multicast group as a result of snooping.";
  }

  identity tf-type {
    description
      "Identity for the traffic type.";
  }
```

```
  identity multicast-traffic {
    base tf-type;
    description
      "Identity for multicast traffic.";
  }

  identity broadcast-traffic {
    base tf-type;
    description
      "Identity for broadcast traffic.";
  }

  identity unknown-unicast-traffic {
    base tf-type;
    description
      "Identity for unknown unicast traffic.";
  }

  identity encapsulation-type {
    description
      "Identity for the encapsulation type.";
  }

  identity ethernet {
    base encapsulation-type;
    description
      "Identity for Ethernet type.";
  }

  identity vlan {
    base encapsulation-type;
    description
      "Identity for the VLAN type.";
  }

  identity carrierscarrier-type {
    description
      "Identity of the CsC type.";
  }

  identity ldp {
    base carrierscarrier-type;
    description
      "Use LDP as the signaling protocol
       between the PE and the CE.";
  }

  identity bgp {
    base carrierscarrier-type;
    description
      "Use BGP (as per RFC 8277) as the signaling protocol
       between the PE and the CE.
       In this case, BGP must also be configured as
       the routing protocol.";
  }

  identity eth-inf-type {
    description
      "Identity of the Ethernet interface type.";
  }

  identity tagged {
    base eth-inf-type;
    description
      "Identity of the tagged interface type.";
  }

  identity untagged {
    base eth-inf-type;
    description
      "Identity of the untagged interface type.";
  }

  identity lag {
    base eth-inf-type;
    description
      "Identity of the LAG interface type.";
  }

  identity bw-type {
    description
      "Identity of the bandwidth type.";
  }

  identity bw-per-cos {
    base bw-type;
```

```
    description
      "Bandwidth is per CoS.";
  }

  identity bw-per-port {
    base bw-type;
    description
      "Bandwidth is per site network access.";
  }

  identity bw-per-site {
    base bw-type;
    description
      "Bandwidth is per site.  It is applicable to
       all the site network accesses within the site.";
  }

  identity bw-per-svc {
    base bw-type;
    description
      "Bandwidth is per VPN service.";
  }

  identity site-vpn-flavor {
    description
      "Base identity for the site VPN service flavor.";
  }

  identity site-vpn-flavor-single {
    base site-vpn-flavor;
    description
      "Identity for the site VPN service flavor.
       Used when the site belongs to only one VPN.";
  }

  identity site-vpn-flavor-multi {
    base site-vpn-flavor;
    description
      "Identity for the site VPN service flavor.
       Used when a logical connection of a site
       belongs to multiple VPNs.";
  }

  identity site-vpn-flavor-nni {
    base site-vpn-flavor;
    description
      "Identity for the site VPN service flavor.
       Used to describe an NNI option A connection.";
  }

  identity service-type {
    description
      "Base identity of the service type.";
  }

  identity vpws {
    base service-type;
    description
      "Point-to-point Virtual Private Wire Service (VPWS)
       service type.";
  }

  identity pwe3 {
    base service-type;
    description
      "Pseudowire Emulation Edge to Edge (PWE3) service type.";
  }

  identity ldp-l2tp-vpls {
    base service-type;
    description
      "LDP-based or L2TP-based multipoint Virtual Private LAN
       Service (VPLS) service type.  This VPLS uses LDP-signaled
       Pseudowires or L2TP-signaled Pseudowires.";
  }

  identity bgp-vpls {
    base service-type;
    description
      "BGP-based multipoint VPLS service type.  This VPLS uses a
       BGP control plane as described in RFCs 4761 and 6624.";
  }

  identity vpws-evpn {
    base service-type;
    description
```

```
      "VPWS service type using Ethernet VPNs (EVPNs)
       as specified in RFC 7432.";
  }

  identity pbb-evpn {
    base service-type;
    description
      "Provider Backbone Bridge (PBB) service type using
       EVPNs as specified in RFC 7432.";
  }

  identity bundling-type {
    description
      "The base identity for the bundling type.  It supports
       multiple CE-VLANs associated with an L2VPN service or
       all CE-VLANs associated with an L2VPN service.";
  }

  identity multi-svc-bundling {
    base bundling-type;
    description
      "Identity for multi-service bundling, i.e.,
       multiple CE-VLAN IDs can be associated with an
       L2VPN service at a site.";
  }

  identity one2one-bundling {
    base bundling-type;
    description
      "Identity for one-to-one service bundling, i.e.,
       each L2VPN can be associated with only one CE-VLAN ID
       at a site.";
  }

  identity all2one-bundling {
    base bundling-type;
    description
      "Identity for all-to-one bundling, i.e., all CE-VLAN IDs
       are mapped to one L2VPN service.";
  }

  identity color-id {
    description
      "Base identity of the color ID.";
  }

  identity color-id-cvlan {
    base color-id;
    description
      "Identity of the color ID based on a CVLAN.";
  }

  identity cos-id {
    description
      "Identity of the CoS ID.";
  }

  identity cos-id-pcp {
    base cos-id;
    description
      "Identity of the CoS ID based on the
       Port Control Protocol (PCP).";
  }

  identity cos-id-dscp {
    base cos-id;
    description
      "Identity of the CoS ID based on DSCP.";
  }

  identity color-type {
    description
      "Identity of color types.";
  }

  identity green {
    base color-type;
    description
      "Identity of the 'green' color type.";
  }

  identity yellow {
    base color-type;
    description
      "Identity of the 'yellow' color type.";
  }
```

```
identity red {
  base color-type;
  description
    "Identity of the 'red' color type.";
}

identity policing {
  description
    "Identity of the type of policing applied.";
}

identity one-rate-two-color {
  base policing;
  description
    "Identity of one-rate, two-color (1R2C).";
}

identity two-rate-three-color {
  base policing;
  description
    "Identity of two-rate, three-color (2R3C).";
}

identity bum-type {
  description
    "Identity of the BUM type.";
}

identity broadcast {
  base bum-type;
  description
    "Identity of broadcast.";
}

identity unicast {
  base bum-type;
  description
    "Identity of unicast.";
}

identity multicast {
  base bum-type;
  description
    "Identity of multicast.";
}

identity loop-prevention-type {
  description
    "Identity of loop prevention.";
}

identity shut {
  base loop-prevention-type;
  description
    "Identity of shut protection.";
}

identity trap {
  base loop-prevention-type;
  description
    "Identity of trap protection.";
}

identity lacp-state {
  description
    "Identity of the LACP state.";
}

identity lacp-on {
  base lacp-state;
  description
    "Identity of LACP on.";
}

identity lacp-off {
  base lacp-state;
  description
    "Identity of LACP off.";
}

identity lacp-mode {
  description
    "Identity of the LACP mode.";
}
```

```
  identity lacp-passive {
    base lacp-mode;
    description
      "Identity of LACP passive.";
  }

  identity lacp-active {
    base lacp-mode;
    description
      "Identity of LACP active.";
  }

  identity lacp-speed {
    description
      "Identity of the LACP speed.";
  }

  identity lacp-fast {
    base lacp-speed;
    description
      "Identity of LACP fast.";
  }

  identity lacp-slow {
    base lacp-speed;
    description
      "Identity of LACP slow.";
  }

  identity bw-direction {
    description
      "Identity for the bandwidth direction.";
  }

  identity input-bw {
    base bw-direction;
    description
      "Identity for the input bandwidth.";
  }

  identity output-bw {
    base bw-direction;
    description
      "Identity for the output bandwidth.";
  }

  identity management {
    description
      "Base identity for the site management scheme.";
  }

  identity co-managed {
    base management;
    description
      "Identity for a co-managed site.";
  }

  identity customer-managed {
    base management;
    description
      "Identity for a customer-managed site.";
  }

  identity provider-managed {
    base management;
    description
      "Identity for a provider-managed site.";
  }

  identity address-family {
    description
      "Identity for an address family.";
  }

  identity ipv4 {
    base address-family;
    description
      "Identity for an IPv4 address family.";
  }

  identity ipv6 {
    base address-family;
    description
      "Identity for an IPv6 address family.";
  }
```

```
  identity vpn-topology {
    description
      "Base identity for the VPN topology.";
  }

  identity any-to-any {
    base vpn-topology;
    description
      "Identity for the any-to-any VPN topology.";
  }

  identity hub-spoke {
    base vpn-topology;
    description
      "Identity for the Hub-and-Spoke VPN topology.";
  }

  identity hub-spoke-disjoint {
    base vpn-topology;
    description
      "Identity for the Hub-and-Spoke VPN topology,
       where Hubs cannot communicate with each other.";
  }

  identity site-role {
    description
      "Base identity for a site type.";
  }

  identity any-to-any-role {
    base site-role;
    description
      "Site in an any-to-any L2VPN.";
  }

  identity spoke-role {
    base site-role;
    description
      "Spoke site in a Hub-and-Spoke L2VPN.";
  }

  identity hub-role {
    base site-role;
    description
      "Hub site in a Hub-and-Spoke L2VPN.";
  }

  identity pm-type {
    description
      "Performance-monitoring type.";
  }

  identity loss {
    base pm-type;
    description
      "Loss measurement.";
  }

  identity delay {
    base pm-type;
    description
      "Delay measurement.";
  }

  identity fault-alarm-defect-type {
    description
      "Indicates the alarm-priority defect (i.e., the
       lowest-priority defect that is allowed to
       generate a fault alarm).";
  }

  identity remote-rdi {
    base fault-alarm-defect-type;
    description
      "Indicates the aggregate health
       of the Remote MEPs.";
  }

  identity remote-mac-error {
    base fault-alarm-defect-type;
    description
      "Indicates that one or more of the Remote MEPs are
       reporting a failure in their Port Status TLVs or
       Interface Status TLVs.";
  }
```

```
  identity remote-invalid-ccm {
    base fault-alarm-defect-type;
    description
      "Indicates that at least one of the Remote MEP
       state machines is not receiving valid
       Continuity Check Messages (CCMs) from its Remote MEP.";
  }

  identity invalid-ccm {
    base fault-alarm-defect-type;
    description
      "Indicates that one or more invalid CCMs have been
       received and that a period of time 3.5 times the length
       of those CCMs' transmission intervals has not yet expired.";
  }

  identity cross-connect-ccm {
    base fault-alarm-defect-type;
    description
      "Indicates that one or more cross-connect CCMs have been
       received and that 3.5 times the period of at least one of
       those CCMs' transmission intervals has not yet expired.";
  }

  identity frame-delivery-mode {
    description
      "Delivery types.";
  }

  identity discard {
    base frame-delivery-mode;
    description
      "Service frames are discarded.";
  }

  identity unconditional {
    base frame-delivery-mode;
    description
      "Service frames are unconditionally delivered to the
       destination site.";
  }

  identity unknown-discard {
    base frame-delivery-mode;
    description
      "Service frames are conditionally delivered to the
       destination site.  Packets with unknown destination addresses
       will be discarded.";
  }

  identity placement-diversity {
    description
      "Base identity for site placement constraints.";
  }

  identity bearer-diverse {
    base placement-diversity;
    description
      "Identity for bearer diversity.
       The bearers should not use common elements.";
  }

  identity pe-diverse {
    base placement-diversity;
    description
      "Identity for PE diversity.";
  }

  identity pop-diverse {
    base placement-diversity;
    description
      "Identity for POP diversity.";
  }

  identity linecard-diverse {
    base placement-diversity;
    description
      "Identity for linecard diversity.";
  }

  identity same-pe {
    base placement-diversity;
    description
      "Identity for having sites connected on the same PE.";
  }
```

```
  identity same-bearer {
    base placement-diversity;
    description
      "Identity for having sites connected using the same bearer.";
  }

  identity tagged-inf-type {
    description
      "Identity for the tagged interface type.";
  }

  identity priority-tagged {
    base tagged-inf-type;
    description
      "Identity for the priority-tagged interface.";
  }

  identity qinq {
    base tagged-inf-type;
    description
      "Identity for the QinQ tagged interface.";
  }

  identity dot1q {
    base tagged-inf-type;
    description
      "Identity for the dot1Q VLAN tagged interface.";
  }

  identity qinany {
    base tagged-inf-type;
    description
      "Identity for the QinAny tagged interface.";
  }

  identity vxlan {
    base tagged-inf-type;
    description
      "Identity for the VXLAN tagged interface.";
  }

  identity provision-model {
    description
      "Base identity for the provision model.";
  }

  identity single-side-provision {
    description
      "Identity for single-sided provisioning with discovery.";
  }

  identity doubled-side-provision {
    description
      "Identity for double-sided provisioning.";
  }

  identity mac-learning-mode {
    description
      "MAC learning mode.";
  }

  identity data-plane {
    base mac-learning-mode;
    description
      "User MAC addresses are learned through ARP broadcast.";
  }

  identity control-plane {
    base mac-learning-mode;
    description
      "User MAC addresses are advertised through EVPN-BGP.";
  }

  identity vpn-policy-filter-type {
    description
      "Base identity for the filter type.";
  }

  identity lan {
    base vpn-policy-filter-type;
    description
      "Identity for a LAN tag filter type.";
  }

  identity mac-action {
    description
```

```
      "Base identity for a MAC action.";
  }

  identity drop {
    base mac-action;
    description
      "Identity for dropping a packet.";
  }

  identity flood {
    base mac-action;
    description
      "Identity for packet flooding.";
  }

  identity warning {
    base mac-action;
    description
      "Identity for sending a warning log message.";
  }

  identity qos-profile-direction {
    description
      "Base identity for the QoS-profile direction.";
   }

  identity site-to-wan {
    base qos-profile-direction;
    description
      "Identity for the site-to-WAN direction.";
  }

  identity wan-to-site {
    base qos-profile-direction;
    description
      "Identity for the WAN-to-site direction.";
  }

  identity bidirectional {
    base qos-profile-direction;
    description
      "Identity for both the WAN-to-site direction
       and the site-to-WAN direction.";
  }

  identity vxlan-peer-mode {
    description
      "Base identity for the VXLAN peer mode.";
  }

  identity static-mode {
    base vxlan-peer-mode;
    description
      "Identity for VXLAN access in the static mode.";
  }

  identity bgp-mode {
    base vxlan-peer-mode;
    description
      "Identity for VXLAN access by BGP EVPN learning.";
  }

  identity customer-application {
    description
      "Base identity for a customer application.";
  }

  identity web {
    base customer-application;
    description
      "Identity for a web application (e.g., HTTP, HTTPS).";
  }

  identity mail {
    base customer-application;
    description
      "Identity for a mail application.";
  }

  identity file-transfer {
    base customer-application;
    description
      "Identity for a file-transfer application
       (e.g., FTP, SFTP).";
  }
```

```
  identity database {
    base customer-application;
    description
      "Identity for a database application.";
  }

  identity social {
    base customer-application;
    description
      "Identity for a social-network application.";
  }

  identity games {
    base customer-application;
    description
      "Identity for a gaming application.";
  }

  identity p2p {
    base customer-application;
    description
      "Identity for a peer-to-peer application.";
  }

  identity network-management {
    base customer-application;
    description
      "Identity for a management application
       (e.g., Telnet, syslog, SNMP).";
  }

  identity voice {
    base customer-application;
    description
      "Identity for a voice application.";
  }

  identity video {
    base customer-application;
    description
      "Identity for a videoconference application.";
  }

  identity embb {
    base customer-application;
    description
      "Identity for the enhanced Mobile Broadband (eMBB)
       application.  Note that the eMBB application
       requires strict threshold values for a wide variety
       of network performance parameters (e.g., data rate,
       latency, loss rate, reliability).";
  }

  identity urllc {
    base customer-application;
    description
      "Identity for the Ultra-Reliable and Low Latency
       Communications (URLLC) application.  Note that the
       URLLC application requires strict threshold values for
       a wide variety of network performance parameters
       (e.g., latency, reliability).";
  }

  identity mmtc {
    base customer-application;
    description
      "Identity for the massive Machine Type
       Communications (mMTC) application.  Note that the
       mMTC application requires strict threshold values for
       a wide variety of network performance parameters
       (e.g., data rate, latency, loss rate, reliability).";
  }

  grouping site-acl {
    container access-control-list {
      if-feature "acl";
      list mac {
        key "mac-address";
        leaf mac-address {
          type yang:mac-address;
          description
            "MAC addresses.";
        }
        description
          "List of MAC addresses.";
      }
```

```
      description
        "Container for the ACL.";
    }
    description
      "Grouping that defines the ACL.";
  }

  grouping site-bum {
    container broadcast-unknown-unicast-multicast {
      if-feature "bum";
      leaf multicast-site-type {
        type enumeration {
          enum receiver-only {
            description
              "The site only has receivers.";
          }
          enum source-only {
            description
              "The site only has sources.";
          }
          enum source-receiver {
            description
              "The site has both sources and receivers.";
          }
        }
        default "source-receiver";
        description
          "Type of multicast site.";
      }
      list multicast-gp-address-mapping {
        key "id";
        leaf id {
          type uint16;
          description
            "Unique identifier for the mapping.";
        }
        leaf vlan-id {
          type uint16 {
            range "0..1024";
          }
          mandatory true;
          description
            "The VLAN ID of the multicast group.
             The range of the 12-bit VLAN ID is 0 to 1024.";
        }
        leaf mac-gp-address {
          type yang:mac-address;
          mandatory true;
          description
            "The MAC address of the multicast group.";
        }
        leaf port-lag-number {
          type uint32;
          description
            "The ports/LAGs belonging to the multicast group.";
        }
        description
          "List of port-to-group mappings.";
      }
      leaf bum-overall-rate {
        type uint64;
        units "bps";
        description
          "Overall rate for BUM.";
      }
      list bum-rate-per-type {
        key "type";
        leaf type {
          type identityref {
            base bum-type;
          }
          description
            "BUM type.";
        }
        leaf rate {
          type uint64;
          units "bps";
          description
            "Rate for BUM.";
        }
        description
          "List of limit rates for the BUM type.";
      }
      description
        "Container of BUM configurations.";
    }
```

```
    description
      "Grouping for BUM.";
  }

  grouping site-mac-loop-prevention {
    container mac-loop-prevention {
      if-feature "mac-loop-prevention";
      leaf protection-type {
        type identityref {
          base loop-prevention-type;
        }
        default "trap";
        description
          "Protection type.  By default, the protection
           type is 'trap'.";
      }
      leaf frequency {
        type uint32;
        default "5";
        description
          "The number of times to detect MAC duplication, where
           a 'duplicate MAC address' situation has occurred and
           the duplicate MAC address has been added to a list of
           duplicate MAC addresses.  By default, the number of
           times is 5.";
      }
      leaf retry-timer {
        type uint32;
        units "seconds";
        description
          "The retry timer.  When the retry timer expires,
           the duplicate MAC address will be flushed from
           the MAC-VRF.";
      }
      description
        "Container of MAC loop-prevention parameters.";
    }
    description
      "Grouping for MAC loop prevention.";
  }

  grouping site-service-qos-profile {
    container qos {
      if-feature "qos";
      container qos-classification-policy {
        list rule {
          key "id";
          ordered-by user;
          leaf id {
            type string;
            description
              "A description identifying the QoS classification
               policy rule.";
          }
          choice match-type {
            default "match-flow";
            case match-flow {
              container match-flow {
                leaf dscp {
                  type inet:dscp;
                  description
                    "DSCP value.";
                }
                leaf dot1q {
                  type uint16;
                  description
                    "802.1Q matching.  It is a VLAN tag added into
                     a frame.";
                }
                leaf pcp {
                  type uint8 {
                    range "0..7";
                  }
                  description
                    "PCP value.";
                }
                leaf src-mac {
                  type yang:mac-address;
                  description
                    "Source MAC.";
                }
                leaf dst-mac {
                  type yang:mac-address;
                  description
                    "Destination MAC.";
                }
```

```
            leaf color-type {
              type identityref {
                base color-type;
              }
              description
                "Color types.";
            }
            leaf-list target-sites {
              if-feature "target-sites";
              type svc-id;
              description
                "Identifies a site as a traffic destination.";
            }
            leaf any {
              type empty;
              description
                "Allow all.";
            }
            leaf vpn-id {
              type svc-id;
              description
                "Reference to the target VPN.";
            }
            description
              "Describes flow-matching criteria.";
          }
        }
        case match-application {
          leaf match-application {
            type identityref {
              base customer-application;
            }
            description
              "Defines the application to match.";
          }
        }
        description
          "Choice for classification.";
      }
      leaf target-class-id {
        type string;
        description
          "Identification of the CoS.
           This identifier is internal to the
           administration.";
      }
      description
        "List of marking rules.";
    }
    description
      "Configuration of the traffic classification policy.";
  }
  container qos-profile {
    choice qos-profile {
      description
        "Choice for the QoS profile.
         Can be a standard profile or a customized profile.";
      case standard {
        description
          "Standard QoS profile.";
        leaf profile {
          type leafref {
            path "/l2vpn-svc/vpn-profiles/"
               + "valid-provider-identifiers/"
               + "qos-profile-identifier";
          }
          description
            "QoS profile to be used.";
        }
      }
      case custom {
        description
          "Customized QoS profile.";
        container classes {
          if-feature "qos-custom";
          list class {
            key "class-id";
            leaf class-id {
              type string;
              description
                "Identification of the CoS.  This identifier is
                 internal to the administration.";
            }
            leaf direction {
              type identityref {
                base qos-profile-direction;
```

```
      }
      default "bidirectional";
      description
        "The direction in which the QoS profile is
         applied.  By default, the direction is
         bidirectional.";
    }
    leaf policing {
      type identityref {
        base policing;
      }
      default "one-rate-two-color";
      description
        "The policing type can be either one-rate,
         two-color (1R2C) or two-rate, three-color
         (2R3C).  By default, the policing type is
         'one-rate-two-color'.";
    }
    leaf byte-offset {
      type uint16;
      description
        "Number of bytes in the service frame header
         that are excluded from the QoS calculation
         (e.g., extra VLAN tags).";
    }
    container frame-delay {
      choice flavor {
        case lowest {
          leaf use-lowest-latency {
            type empty;
            description
              "The traffic class should use the path
               with the lowest delay.";
          }
        }
        case boundary {
          leaf delay-bound {
            type uint16;
            units "milliseconds";
            description
              "The traffic class should use a path
               with a defined maximum delay.";
          }
        }
        description
          "Delay constraint on the traffic class.";
      }
      description
        "Delay constraint on the traffic class.";
    }
    container frame-jitter {
      choice flavor {
        case lowest {
          leaf use-lowest-jitter {
            type empty;
            description
              "The traffic class should use the path
               with the lowest jitter.";
          }
        }
        case boundary {
          leaf delay-bound {
            type uint32;
            units "microseconds";
            description
              "The traffic class should use a path
               with a defined maximum jitter.";
          }
        }
        description
          "Jitter constraint on the traffic class.";
      }
      description
        "Jitter constraint on the traffic class.";
    }
    container frame-loss {
      leaf rate {
        type decimal64 {
          fraction-digits 2;
          range "0..100";
        }
        units "percent";
        description
          "Frame loss rate constraint on the traffic
           class.";
      }
```

```
                description
                  "Container for frame loss rate.";
              }
              container bandwidth {
                leaf guaranteed-bw-percent {
                  type decimal64 {
                    fraction-digits 5;
                    range "0..100";
                  }
                  units "percent";
                  mandatory true;
                  description
                    "Used to define the guaranteed bandwidth
                     as a percentage of the available service
                     bandwidth.";
                }
                leaf end-to-end {
                  type empty;
                  description
                    "Used if the bandwidth reservation
                     must be done on the MPLS network too.";
                }
                description
                  "Bandwidth constraint on the traffic class.";
              }
              description
                "List of CoS entries.";
            }
            description
              "Container for list of CoS entries.";
          }
        }
      }
      description
        "Qos profile configuration.";
    }
    description
      "QoS configuration.";
  }
  description
    "Grouping that defines QoS parameters for a site.";
}

grouping site-service-mpls {
  container carrierscarrier {
    if-feature "carrierscarrier";
    leaf signaling-type {
      type identityref {
        base carrierscarrier-type;
      }
      default "bgp";
      description
        "CsC.  By default, the signaling type is 'bgp'.";
    }
    description
      "Container for CsC.";
  }
  description
    "Grouping for CsC.";
}

container l2vpn-svc {
  container vpn-profiles {
    container valid-provider-identifiers {
      leaf-list cloud-identifier {
        if-feature "cloud-access";
        type string;
        description
          "Identification of the public cloud service or
           Internet service.  Local to each administration.";
      }
      leaf-list qos-profile-identifier {
        type string;
        description
          "Identification of the QoS profile to be used.
           Local to each administration.";
      }
      leaf-list bfd-profile-identifier {
        type string;
        description
          "Identification of the SP BFD profile to be used.
           Local to each administration.";
      }
      leaf-list remote-carrier-identifier {
        type string;
        description
```

```
            "Identification of the remote carrier name to be used.
             It can be an L2VPN partner, data-center SP, or
             private CSP.  Local to each administration.";
        }
        nacm:default-deny-write;
        description
          "Container for valid provider identifiers.";
      }
      description
        "Container for VPN profiles.";
    }
    container vpn-services {
      list vpn-service {
        key "vpn-id";
        leaf vpn-id {
          type svc-id;
          description
            "Defines a service identifier.";
        }
        leaf vpn-svc-type {
          type identityref {
            base service-type;
          }
          default "vpws";
          description
            "Service type.  By default, the service type is 'vpws'.";
        }
        leaf customer-name {
          type string;
          description
            "Customer name.";
        }
        leaf svc-topo {
          type identityref {
            base vpn-topology;
          }
          default "any-to-any";
          description
            "Defines the service topology, e.g.,
             'any-to-any', 'hub-spoke'.";
        }
        container cloud-accesses {
          if-feature "cloud-access";
          list cloud-access {
            key "cloud-identifier";
            leaf cloud-identifier {
              type leafref {
                path "/l2vpn-svc/vpn-profiles/"
                   + "valid-provider-identifiers"
                   + "/cloud-identifier";
              }
              description
                "Identification of the cloud service.
                 Local to each administration.";
            }
            choice list-flavor {
              case permit-any {
                leaf permit-any {
                  type empty;
                  description
                    "Allow all sites.";
                }
              }
              case deny-any-except {
                leaf-list permit-site {
                  type leafref {
                    path "/l2vpn-svc/sites/site/site-id";
                  }
                  description
                    "Site ID to be authorized.";
                }
              }
              case permit-any-except {
                leaf-list deny-site {
                  type leafref {
                    path "/l2vpn-svc/sites/site/site-id";
                  }
                  description
                    "Site ID to be denied.";
                }
              }
              description
                "Choice for cloud access policy.
                 By default, all sites in the L2VPN
                 MUST be authorized to access the cloud.";
            }
```

```
        description
          "Cloud access configuration.";
      }
      description
        "Container for cloud access configurations.";
    }
    container frame-delivery {
      if-feature "bum";
      container customer-tree-flavors {
        leaf-list tree-flavor {
          type identityref {
            base multicast-tree-type;
          }
          description
            "Type of tree to be used.";
        }
        description
          "Types of trees used by the customer.";
      }
      container bum-deliveries {
        list bum-delivery {
          key "frame-type";
          leaf frame-type {
            type identityref {
              base tf-type;
            }
            description
              "Type of frame delivery.  It supports unicast
               frame delivery, multicast frame delivery,
               and broadcast frame delivery.";
          }
          leaf delivery-mode {
            type identityref {
              base frame-delivery-mode;
            }
            default "unconditional";
            description
              "Defines the frame delivery mode
               ('unconditional' (default), 'conditional',
               or 'discard').  By default, service frames are
               unconditionally delivered to the destination site.";
          }
          description
            "List of frame delivery types and modes.";
        }
        description
          "Defines the frame delivery types and modes.";
      }
      leaf multicast-gp-port-mapping {
        type identityref {
          base multicast-gp-address-mapping;
        }
        mandatory true;
        description
          "Describes the way in which each interface is
           associated with the multicast group.";
      }
      description
        "Multicast global parameters for the VPN service.";
    }
    container extranet-vpns {
      if-feature "extranet-vpn";
      list extranet-vpn {
        key "vpn-id";
        leaf vpn-id {
          type svc-id;
          description
            "Identifies the target VPN that the local VPN wants to
             access.";
        }
        leaf local-sites-role {
          type identityref {
            base site-role;
          }
          default "any-to-any-role";
          description
            "Describes the role of the local sites in the target
             VPN topology.  In the any-to-any VPN service topology,
             the local sites must have the same role, which will be
             'any-to-any-role'.  In the Hub-and-Spoke VPN service
             topology or the Hub-and-Spoke-Disjoint VPN service
             topology, the local sites must have a Hub role or a
             Spoke role.";
        }
        description
          "List of extranet VPNs to which the local VPN
```

```
              is attached.";
          }
          description
            "Container for extranet VPN configurations.";
        }
        leaf ce-vlan-preservation {
          type boolean;
          mandatory true;
          description
            "Preserves the CE-VLAN ID from ingress to egress, i.e.,
             the CE-VLAN tag of the egress frame is identical to
             that of the ingress frame that yielded this
             egress service frame.  If all-to-one bundling within
             a site is enabled, then preservation applies to all
             ingress service frames.  If all-to-one bundling is
             disabled, then preservation applies to tagged
             ingress service frames having CE-VLAN IDs 1 through 4094.";
        }
        leaf ce-vlan-cos-preservation {
          type boolean;
          mandatory true;
          description
            "CE VLAN CoS preservation.  The PCP bits in the CE-VLAN tag
             of the egress frame are identical to those of the
             ingress frame that yielded this egress service frame.";
        }
        leaf carrierscarrier {
          if-feature "carrierscarrier";
          type boolean;
          default "false";
          description
            "The VPN is using CsC, and so MPLS is required.";
        }
        description
          "List of VPN services.";
      }
      description
        "Container for VPN services.";
    }
    container sites {
      list site {
        key "site-id";
        leaf site-id {
          type string;
          description
            "Identifier of the site.";
        }
        leaf site-vpn-flavor {
          type identityref {
            base site-vpn-flavor;
          }
          default "site-vpn-flavor-single";
          description
            "Defines the way that the VPN multiplexing is
             done, e.g., whether the site belongs to
             a single VPN site or a multi-VPN site.  By
             default, the site belongs to a single VPN.";
        }
        container devices {
          when "derived-from-or-self(../management/type, "
             + "'l2vpn-svc:provider-managed') or "
             + "derived-from-or-self(../management/type, "
             + "'l2vpn-svc:co-managed')" {
            description
              "Applicable only for a provider-managed or
               co-managed device.";
          }
          list device {
            key "device-id";
            leaf device-id {
              type string;
              description
                "Identifier for the device.";
            }
            leaf location {
              type leafref {
                path "../../../locations/location/location-id";
              }
              mandatory true;
              description
                "Location of the device.";
            }
            container management {
              when "derived-from-or-self(../../../management/type, "
                 + "'l2vpn-svc:co-managed')" {
                description
```

```
            "Applicable only for a co-managed device.";
        }
        leaf transport {
          type identityref {
            base address-family;
          }
          description
            "Transport protocol or address family
             used for management.";
        }
        leaf address {
          when '(../ transport)' {
            description
              "If the address family is specified, then the
               address should also be specified.  If the
               transport is not specified, then the address
               should not be specified.";
          }
          type inet:ip-address;
          description
            "Management address.";
        }
        description
          "Management configuration.  Applicable only for a
           co-managed device.";
      }
      description
        "List of devices requested by the customer.";
    }
    description
      "Device configurations.";
  }
  container management {
    leaf type {
      type identityref {
        base management;
      }
      mandatory true;
      description
        "Management type of the connection.";
    }
    description
      "Management configuration.";
  }
  container locations {
    list location {
      key "location-id";
      leaf location-id {
        type string;
        description
          "Location ID.";
      }
      leaf address {
        type string;
        description
          "Address (number and street) of the site.";
      }
      leaf postal-code {
        type string;
        description
          "Postal code of the site.  The format of 'postal-code'
           is similar to the 'PC' (postal code) label format
           defined in RFC 4119.";
      }
      leaf state {
        type string;
        description
          "State (region) of the site.  This leaf can also be used
           to describe a region of a country that does not have
           states.";
      }
      leaf city {
        type string;
        description
          "City of the site.";
      }
      leaf country-code {
        type string;
        description
          "Country of the site.  The format of 'country-code' is
           similar to the 'country' label defined in RFC 4119.";
      }
      description
        "List of locations.";
    }
    description
```

```
          "Location of the site.";
      }
      container site-diversity {
        if-feature "site-diversity";
        container groups {
          list group {
            key "group-id";
            leaf group-id {
              type string;
              description
                "The group-id to which the site belongs.";
            }
            description
              "List of group-ids.";
          }
          description
            "Groups to which the site belongs.
             All site network accesses will inherit those group
             values.";
        }
        description
          "The type of diversity constraint.";
      }
      container vpn-policies {
        list vpn-policy {
          key "vpn-policy-id";
          leaf vpn-policy-id {
            type string;
            description
              "Unique identifier for the VPN policy.";
          }
          list entries {
            key "id";
            leaf id {
              type string;
              description
                "Unique identifier for the policy entry.";
            }
            container filters {
              list filter {
                key "type";
                ordered-by user;
                leaf type {
                  type identityref {
                    base vpn-policy-filter-type;
                  }
                  description
                    "Type of VPN policy filter.";
                }
                leaf-list lan-tag {
                  when "derived-from-or-self(../type, "
                     + "'l2vpn-svc:lan')" {
                    description
                      "Only applies when the VPN policy filter is a
                       LAN tag filter.";
                  }
                  if-feature "lan-tag";
                  type uint32;
                  description
                    "List of Ethernet LAN tags to be matched.  An
                     Ethernet LAN tag identifies a particular
                     broadcast domain in a VPN.";
                }
                description
                  "List of filters used on the site.  This list can
                   be augmented.";
              }
              description
                "If a more granular VPN attachment is necessary,
                 filtering can be used.  If used, it permits the
                 splitting of site LANs among multiple VPNs.  The
                 site LAN can be split based on either the LAN tag or
                 the LAN prefix.  If no filter is used, all the LANs
                 will be part of the same VPNs with the same role.";
            }
            list vpn {
              key "vpn-id";
              leaf vpn-id {
                type leafref {
                  path "/l2vpn-svc/vpn-services/vpn-service/vpn-id";
                }
                description
                  "Reference to an L2VPN.";
              }
              leaf site-role {
                type identityref {
```

```
                base site-role;
              }
              default "any-to-any-role";
              description
                "Role of the site in the L2VPN.";
            }
            description
              "List of VPNs with which the LAN is associated.";
          }
          description
            "List of entries for an export policy.";
        }
        description
          "List of VPN policies.";
      }
      description
        "VPN policy.";
    }
    container service {
      uses site-service-qos-profile;
      uses site-service-mpls;
      description
        "Service parameters on the attachment.";
    }
    uses site-bum;
    uses site-mac-loop-prevention;
    uses site-acl;
    leaf actual-site-start {
      type yang:date-and-time;
      config false;
      description
        "This leaf is optional.  It indicates the date and time
         when the service at a particular site actually started.";
    }
    leaf actual-site-stop {
      type yang:date-and-time;
      config false;
      description
        "This leaf is optional.  It indicates the date and time
         when the service at a particular site actually stopped.";
    }
    leaf bundling-type {
      type identityref {
        base bundling-type;
      }
      default "one2one-bundling";
      description
        "Bundling type.  By default, each L2VPN
         can be associated with only one
         CE-VLAN, i.e., one-to-one bundling is used.";
    }
    leaf default-ce-vlan-id {
      type uint32;
      mandatory true;
      description
        "Default CE VLAN ID set at the site level.";
    }
    container site-network-accesses {
      list site-network-access {
        key "network-access-id";
        leaf network-access-id {
          type string;
          description
            "Identifier of network access.";
        }
        leaf remote-carrier-name {
          when "derived-from-or-self(../../../site-vpn-flavor,"
             + "'l2vpn-svc:site-vpn-flavor-nni')" {
            description
              "Relevant when the site's VPN flavor is
               'site-vpn-flavor-nni'.";
          }
          type leafref {
            path "/l2vpn-svc/vpn-profiles/"
               + "valid-provider-identifiers"
               + "/remote-carrier-identifier";
          }
          description
            "Remote carrier name.  The 'remote-carrier-name'
             parameter must be configured only when
             'site-vpn-flavor' is set to 'site-vpn-flavor-nni'.
             If it is not set, it indicates that the customer
             does not know the remote carrier's name
             beforehand.";
        }
        leaf type {
```

```
        type identityref {
          base site-network-access-type;
        }
        default "point-to-point";
        description
          "Describes the type of connection, e.g.,
           point-to-point or multipoint.";
      }
      choice location-flavor {
        case location {
          when "derived-from-or-self(../../management/type, "
             + "'l2vpn-svc:customer-managed')" {
            description
              "Applicable only for a customer-managed device.";
          }
          leaf location-reference {
            type leafref {
              path "../../../locations/location/location-id";
            }
            description
              "Location of the site-network-access.";
          }
        }
        case device {
          when "derived-from-or-self(../../management/type, "
             + "'l2vpn-svc:provider-managed') or "
             + "derived-from-or-self(../../management/type, "
             + "'l2vpn-svc:co-managed')" {
            description
              "Applicable only for a provider-managed
               or co-managed device.";
          }
          leaf device-reference {
            type leafref {
              path "../../../devices/device/device-id";
            }
            description
              "Identifier of the CE to use.";
          }
        }
        mandatory true;
        description
          "Choice of how to describe the site's location.";
      }
      container access-diversity {
        if-feature "site-diversity";
        container groups {
          list group {
            key "group-id";
            leaf group-id {
              type string;
              description
                "Group-id to which the site belongs.";
            }
            description
              "List of group-ids.";
          }
          description
            "Groups to which the site or site-network-access
             belongs.";
        }
        container constraints {
          list constraint {
            key "constraint-type";
            leaf constraint-type {
              type identityref {
                base placement-diversity;
              }
              description
                "The type of diversity constraint.";
            }
            container target {
              choice target-flavor {
                default "id";
                case id {
                  list group {
                    key "group-id";
                    leaf group-id {
                      type string;
                      description
                        "The constraint will apply against this
                         particular group-id.";
                    }
                    description
                      "List of groups.";
                  }
```

```
            }
            case all-accesses {
              leaf all-other-accesses {
                type empty;
                description
                  "The constraint will apply against all other
                   site network accesses of this site.";
              }
            }
            case all-groups {
              leaf all-other-groups {
                type empty;
                description
                  "The constraint will apply against all other
                   groups the customer is managing.";
              }
            }
            description
              "Choice for the group definition.";
          }
          description
            "The constraint will apply against
             this list of groups.";
        }
        description
          "List of constraints.";
      }
      description
        "Constraints for placing this site network access.";
    }
    description
      "Diversity parameters.";
  }
  container bearer {
    container requested-type {
      if-feature "requested-type";
      leaf type {
        type string;
        description
          "Type of requested bearer: Ethernet, ATM, Frame
           Relay, IP Layer 2 transport, Frame Relay Data
           Link Connection Identifier (DLCI), SONET/SDH,
           PPP.";
      }
      leaf strict {
        type boolean;
        default "false";
        description
          "Defines whether the requested type is a preference
           or a strict requirement.";
      }
      description
        "Container for requested types.";
    }
    leaf always-on {
      if-feature "always-on";
      type boolean;
      default "true";
      description
        "Request for an 'always-on' access type.
         For example, this could mean no dial-in access
         type.";
    }
    leaf bearer-reference {
      if-feature "bearer-reference";
      type string;
      description
        "An internal reference for the SP.";
    }
    description
      "Bearer-specific parameters.  To be augmented.";
  }
  container connection {
    leaf encapsulation-type {
      type identityref {
        base encapsulation-type;
      }
      default "ethernet";
      description
        "Encapsulation type.  By default, the
         encapsulation type is set to 'ethernet'.";
    }
    leaf eth-inf-type {
      type identityref {
        base eth-inf-type;
      }
```

```
        default "untagged";
        description
          "Ethernet interface type.  By default, the
           Ethernet interface type is set to 'untagged'.";
      }
      container tagged-interface {
        leaf type {
          type identityref {
            base tagged-inf-type;
          }
          default "priority-tagged";
          description
            "Tagged interface type.  By default,
             the type of the tagged interface is
             'priority-tagged'.";
        }
        container dot1q-vlan-tagged {
          when "derived-from-or-self(../type, "
             + "'l2vpn-svc:dot1q')" {
            description
              "Only applies when the type of the tagged
               interface is 'dot1q'.";
          }
          if-feature "dot1q";
          leaf tg-type {
            type identityref {
              base tag-type;
            }
            default "c-vlan";
            description
              "Tag type.  By default, the tag type is
               'c-vlan'.";
          }
          leaf cvlan-id {
            type uint16;
            mandatory true;
            description
              "VLAN identifier.";
          }
          description
            "Tagged interface.";
        }
        container priority-tagged {
          when "derived-from-or-self(../type, "
             + "'l2vpn-svc:priority-tagged')" {
            description
              "Only applies when the type of the tagged
               interface is 'priority-tagged'.";
          }
          leaf tag-type {
            type identityref {
              base tag-type;
            }
            default "c-vlan";
            description
              "Tag type.  By default, the tag type is
               'c-vlan'.";
          }
          description
            "Priority tagged.";
        }
        container qinq {
          when "derived-from-or-self(../type, "
             + "'l2vpn-svc:qinq')" {
            description
              "Only applies when the type of the tagged
               interface is 'qinq'.";
          }
          if-feature "qinq";
          leaf tag-type {
            type identityref {
              base tag-type;
            }
            default "c-s-vlan";
            description
              "Tag type.  By default, the tag type is
               'c-s-vlan'.";
          }
          leaf svlan-id {
            type uint16;
            mandatory true;
            description
              "SVLAN identifier.";
          }
          leaf cvlan-id {
            type uint16;
```

```
          mandatory true;
          description
            "CVLAN identifier.";
        }
        description
          "QinQ.";
      }
      container qinany {
        when "derived-from-or-self(../type, "
           + "'l2vpn-svc:qinany')" {
        description
          "Only applies when the type of the tagged
           interface is 'qinany'.";
        }
        if-feature "qinany";
        leaf tag-type {
          type identityref {
            base tag-type;
          }
          default "s-vlan";
          description
            "Tag type.  By default, the tag type is
             's-vlan'.";
        }
        leaf svlan-id {
          type uint16;
          mandatory true;
          description
            "SVLAN ID.";
        }
        description
          "Container for QinAny.";
      }
      container vxlan {
        when "derived-from-or-self(../type, "
           + "'l2vpn-svc:vxlan')" {
          description
            "Only applies when the type of the tagged
             interface is 'vxlan'.";
        }
        if-feature "vxlan";
        leaf vni-id {
          type uint32;
          mandatory true;
          description
            "VXLAN Network Identifier (VNI).";
        }
        leaf peer-mode {
          type identityref {
            base vxlan-peer-mode;
          }
          default "static-mode";
          description
            "Specifies the VXLAN access mode.  By default,
             the peer mode is set to 'static-mode'.";
        }
        list peer-list {
          key "peer-ip";
          leaf peer-ip {
            type inet:ip-address;
            description
              "Peer IP.";
          }
          description
            "List of peer IP addresses.";
        }
        description
          "QinQ.";
      }
      description
        "Container for tagged interfaces.";
    }
    container untagged-interface {
      leaf speed {
        type uint32;
        units "mbps";
        default "10";
        description
          "Port speed.";
      }
      leaf mode {
        type neg-mode;
        default "auto-neg";
        description
          "Negotiation mode.";
      }
```

```
        leaf phy-mtu {
          type uint32;
          units "bytes";
          description
            "PHY MTU.";
        }
        leaf lldp {
          type boolean;
          default "false";
          description
            "LLDP.  Indicates that LLDP is supported.";
        }
        container oam-802.3ah-link {
          if-feature "oam-3ah";
          leaf enabled {
            type boolean;
            default "false";
            description
              "Indicates whether or not to support
               OAM 802.3ah links.";
          }
          description
            "Container for OAM 802.3ah links.";
        }
        leaf uni-loop-prevention {
          type boolean;
          default "false";
          description
            "If this leaf is set to 'true', then the port
             automatically goes down when a physical
             loopback is detected.";
        }
        description
          "Container of untagged interface attribute
           configurations.";
      }
      container lag-interfaces {
        if-feature "lag-interface";
        list lag-interface {
          key "index";
          leaf index {
            type string;
            description
              "LAG interface index.";
          }
          container lacp {
            if-feature "lacp";
            leaf enabled {
              type boolean;
              default "false";
              description
                "LACP on/off.  By default, LACP is disabled.";
            }
            leaf mode {
              type neg-mode;
              description
                "LACP mode.  LACP modes have active mode and
                 passive mode ('false').  'Active mode' means
                 initiating the auto-speed negotiation and
                 trying to form an Ethernet channel with the
                 other end.  'Passive mode' means not initiating
                 the negotiation but responding to LACP packets
                 initiated by the other end (e.g., full duplex
                 or half duplex).";
            }
            leaf speed {
              type uint32;
              units "mbps";
              default "10";
              description
                "LACP speed.  By default, the LACP speed is 10
                 Mbps.";
            }
            leaf mini-link-num {
              type uint32;
              description
                "Defines the minimum number of links that must
                 be active before the aggregating link is put
                 into service.";
            }
            leaf system-priority {
              type uint16;
              default "32768";
              description
                "Indicates the LACP priority for the system.
                 The range is from 0 to 65535.
```

```
        The default is 32768.";
    }
    container micro-bfd {
      if-feature "micro-bfd";
      leaf enabled {
        type enumeration {
          enum on {
            description
              "Micro-bfd on.";
          }
          enum off {
            description
              "Micro-bfd off.";
          }
        }
        default "off";
        description
          "Micro-BFD on/off.  By default, micro-BFD
           is set to 'off'.";
      }
      leaf interval {
        type uint32;
        units "milliseconds";
        description
          "BFD interval.";
      }
      leaf hold-timer {
        type uint32;
        units "milliseconds";
        description
          "BFD hold timer.";
      }
      description
        "Container of micro-BFD configurations.";
    }
    container bfd {
      if-feature "bfd";
      leaf enabled {
        type boolean;
        default "false";
        description
          "BFD activation.  By default, BFD is not
           activated.";
      }
      choice holdtime {
        default "fixed";
        case profile {
          leaf profile-name {
            type leafref {
              path "/l2vpn-svc/vpn-profiles/"
                 + "valid-provider-identifiers"
                 + "/bfd-profile-identifier";
            }
            description
              "SP well-known profile.";
          }
          description
            "SP well-known profile.";
        }
        case fixed {
          leaf fixed-value {
            type uint32;
            units "milliseconds";
            description
              "Expected hold time expressed in
               milliseconds.";
          }
        }
        description
          "Choice for the hold-time flavor.";
      }
      description
        "Container for BFD.";
    }
    container member-links {
      list member-link {
        key "name";
        leaf name {
          type string;
          description
            "Member link name.";
        }
        leaf speed {
          type uint32;
          units "mbps";
          default "10";
```

```
                description
                  "Port speed.";
              }
              leaf mode {
                type neg-mode;
                default "auto-neg";
                description
                  "Negotiation mode.";
              }
              leaf link-mtu {
                type uint32;
                units "bytes";
                description
                  "Link MTU size.";
              }
              container oam-802.3ah-link {
                if-feature "oam-3ah";
                leaf enabled {
                  type boolean;
                  default "false";
                  description
                    "Indicates whether OAM 802.3ah links are
                     supported.";
                }
                description
                  "Container for OAM 802.3ah links.";
              }
              description
                "Member link.";
            }
            description
              "Container of the member link list.";
          }
          leaf flow-control {
            type boolean;
            default "false";
            description
              "Flow control.  Indicates whether flow control
               is supported.";
          }
          leaf lldp {
            type boolean;
            default "false";
            description
              "LLDP.  Indicates whether LLDP is supported.";
          }
          description
            "LACP.";
        }
        description
          "List of LAG interfaces.";
      }
      description
        "Container of LAG interface attribute
         configurations.";
    }
    list cvlan-id-to-svc-map {
      key "svc-id";
      leaf svc-id {
        type leafref {
          path "/l2vpn-svc/vpn-services/vpn-service/vpn-id";
        }
        description
          "VPN service identifier.";
      }
      list cvlan-id {
        key "vid";
        leaf vid {
          type uint16;
          description
            "CVLAN ID.";
        }
        description
          "List of CVLAN-ID-to-SVC-map configurations.";
      }
      description
        "List of CVLAN-ID-to-L2VPN-service-map
         configurations.";
    }
    container l2cp-control {
      if-feature "l2cp-control";
      leaf stp-rstp-mstp {
        type control-mode;
        description
          "STP / Rapid STP (RSTP) / Multiple STP (MSTP)
           protocol type applicable to all sites.";
```

```
      }
      leaf pause {
        type control-mode;
        description
          "Pause protocol type applicable to all sites.";
      }
      leaf lacp-lamp {
        type control-mode;
        description
          "LACP / Link Aggregation Marker Protocol (LAMP).";
      }
      leaf link-oam {
        type control-mode;
        description
          "Link OAM.";
      }
      leaf esmc {
        type control-mode;
        description
          "Ethernet Synchronization Messaging Channel
           (ESMC).";
      }
      leaf l2cp-802.1x {
        type control-mode;
        description
          "IEEE 802.1x.";
      }
      leaf e-lmi {
        type control-mode;
        description
          "E-LMI.";
      }
      leaf lldp {
        type boolean;
        description
          "LLDP protocol type applicable to all sites.";
      }
      leaf ptp-peer-delay {
        type control-mode;
        description
          "Precision Time Protocol (PTP) peer delay.";
      }
      leaf garp-mrp {
        type control-mode;
        description
          "GARP/MRP.";
      }
      description
        "Container of L2CP control configurations.";
    }
    container oam {
      if-feature "ethernet-oam";
      leaf md-name {
        type string;
        mandatory true;
        description
          "Maintenance domain name.";
      }
      leaf md-level {
        type uint16 {
          range "0..255";
        }
        mandatory true;
        description
          "Maintenance domain level.  The level may be
           restricted in certain protocols (e.g.,
           protocols in Layer 0 to Layer 7).";
      }
      list cfm-8021-ag {
        if-feature "cfm";
        key "maid";
        leaf maid {
          type string;
          mandatory true;
          description
            "Identifies a Maintenance Association (MA).";
        }
        leaf mep-id {
          type uint32;
          description
            "Local Maintenance Entity Group End Point (MEP)
             ID.  The non-existence of this leaf means
             that no defects are to be reported.";
        }
        leaf mep-level {
          type uint32;
```

```
        description
          "Defines the MEP level.  The non-existence of this
           leaf means that no defects are to be reported.";
      }
      leaf mep-up-down {
        type enumeration {
          enum up {
            description
              "MEP up.";
          }
          enum down {
            description
              "MEP down.";
          }
        }
        default "up";
        description
          "MEP up/down.  By default, MEP up is used.
           The non-existence of this leaf means that
           no defects are to be reported.";
      }
      leaf remote-mep-id {
        type uint32;
        description
          "Remote MEP ID.  The non-existence of this leaf
           means that no defects are to be reported.";
      }
      leaf cos-for-cfm-pdus {
        type uint32;
        description
          "CoS for CFM PDUs.  The non-existence of this leaf
           means that no defects are to be reported.";
      }
      leaf ccm-interval {
        type uint32;
        units "milliseconds";
        default "10000";
        description
          "CCM interval.  By default, the CCM interval is
           10,000 milliseconds (10 seconds).";
      }
      leaf ccm-holdtime {
        type uint32;
        units "milliseconds";
        default "35000";
        description
          "CCM hold time.  By default, the CCM hold time
           is 3.5 times the CCM interval.";
      }
      leaf alarm-priority-defect {
        type identityref {
          base fault-alarm-defect-type;
        }
        default "remote-invalid-ccm";
        description
          "The lowest-priority defect that is
           allowed to generate a fault alarm.  By default,
           'fault-alarm-defect-type' is set to
           'remote-invalid-ccm'.  The non-existence of
           this leaf means that no defects are
           to be reported.";
      }
      leaf ccm-p-bits-pri {
        type ccm-priority-type;
        description
          "The priority parameter for CCMs transmitted by
           the MEP.  The non-existence of this leaf means
           that no defects are to be reported.";
      }
      description
        "List of 802.1ag CFM attributes.";
    }
    list y-1731 {
      if-feature "y-1731";
      key "maid";
      leaf maid {
        type string;
        mandatory true;
        description
          "Identifies an MA.";
      }
      leaf mep-id {
        type uint32;
        description
          "Local MEP ID.  The non-existence of this leaf
           means that no measurements are to be reported.";
```

```
        }
        leaf type {
          type identityref {
            base pm-type;
          }
          default "delay";
          description
            "Performance-monitoring types.  By default, the
             performance-monitoring type is set to 'delay'.
             The non-existence of this leaf means that no
             measurements are to be reported.";
        }
        leaf remote-mep-id {
          type uint32;
          description
            "Remote MEP ID.  The non-existence of this
             leaf means that no measurements are to be
             reported.";
        }
        leaf message-period {
          type uint32;
          units "milliseconds";
          default "10000";
          description
            "Defines the interval between Y.1731
             performance-monitoring messages.  The message
             period is expressed in milliseconds.";
        }
        leaf measurement-interval {
          type uint32;
          units "seconds";
          description
            "Specifies the measurement interval for
             statistics.  The measurement interval is
             expressed in seconds.";
        }
        leaf cos {
          type uint32;
          description
            "CoS.  The non-existence of this leaf means that
             no measurements are to be reported.";
        }
        leaf loss-measurement {
          type boolean;
          default "false";
          description
            "Indicates whether or not to enable loss
             measurement.  By default, loss
             measurement is not enabled.";
        }
        leaf synthetic-loss-measurement {
          type boolean;
          default "false";
          description
            "Indicates whether or not to enable synthetic loss
             measurement.  By default, synthetic loss
             measurement is not enabled.";
        }
        container delay-measurement {
          leaf enable-dm {
            type boolean;
            default "false";
            description
              "Indicates whether or not to enable delay
               measurement.  By default, delay measurement
               is not enabled.";
          }
          leaf two-way {
            type boolean;
            default "false";
            description
              "Indicates whether delay measurement is two-way
               ('true') or one-way ('false').  By default,
               one-way measurement is enabled.";
          }
          description
            "Container for delay measurement.";
        }
        leaf frame-size {
          type uint32;
          units "bytes";
          description
            "Frame size.  The non-existence of this leaf
             means that no measurements are to be reported.";
        }
        leaf session-type {
```

```
            type enumeration {
              enum proactive {
                description
                  "Proactive mode.";
              }
              enum on-demand {
                description
                  "On-demand mode.";
              }
            }
            default "on-demand";
            description
              "Session type.  By default, the session type
               is 'on-demand'.  The non-existence of this
               leaf means that no measurements are to be
               reported.";
          }
          description
            "List of configured Y-1731 instances.";
        }
        description
          "Container for Ethernet Service OAM.";
      }
      description
        "Container for connection requirements.";
    }
    container availability {
      leaf access-priority {
        type uint32;
        default "100";
        description
          "Access priority.  The higher the access-priority
           value, the higher the preference will be for the
           access in question.";
      }
      choice redundancy-mode {
        case single-active {
          leaf single-active {
            type empty;
            description
              "Single-active mode.";
          }
          description
            "In single-active mode, only one node forwards
             traffic to and from the Ethernet segment.";
        }
        case all-active {
          leaf all-active {
            type empty;
            description
              "All-active mode.";
          }
          description
            "In all-active mode, all nodes can forward
             traffic.";
        }
        description
          "Redundancy mode choice.";
      }
      description
        "Container of available optional configurations.";
    }
    container vpn-attachment {
      choice attachment-flavor {
        case vpn-id {
          leaf vpn-id {
            type leafref {
              path "/l2vpn-svc/vpn-services/vpn-service/vpn-id";
            }
            description
              "Reference to an L2VPN.  Referencing a vpn-id
               provides an easy way to attach a particular
               logical access to a VPN.  In this case,
               the vpn-id must be configured.";
          }
          leaf site-role {
            type identityref {
              base site-role;
            }
            default "any-to-any-role";
            description
              "Role of the site in the L2VPN.  When referencing
               a vpn-id, the site-role setting must be added to
               express the role of the site in the target VPN
               service topology.";
          }
```

```
        }
        case vpn-policy-id {
          leaf vpn-policy-id {
            type leafref {
              path "../../../../vpn-policies/vpn-policy/"
                 + "vpn-policy-id";
            }
            description
              "Reference to a VPN policy.";
          }
        }
        mandatory true;
        description
          "Choice for the VPN attachment flavor.";
      }
      description
        "Defines the VPN attachment of a site.";
    }
    container service {
      container svc-bandwidth {
        if-feature "input-bw";
        list bandwidth {
          key "direction type";
          leaf direction {
            type identityref {
              base bw-direction;
            }
            description
              "Indicates the bandwidth direction.  It can be
               the bandwidth download direction from the SP to
               the site or the bandwidth upload direction from
               the site to the SP.";
          }
          leaf type {
            type identityref {
              base bw-type;
            }
            description
              "Bandwidth type.  By default, the bandwidth type
               is set to 'bw-per-cos'.";
          }
          leaf cos-id {
            when "derived-from-or-self(../type, "
               + "'l2vpn-svc:bw-per-cos')" {
              description
                "Relevant when the bandwidth type is set to
                 'bw-per-cos'.";
            }
            type uint8;
            description
              "Identifier of the CoS, indicated by DSCP or a
               CE-VLAN CoS (802.1p) value in the service frame.
               If the bandwidth type is set to 'bw-per-cos',
               the CoS ID MUST also be specified.";
          }
          leaf vpn-id {
            when "derived-from-or-self(../type, "
               + "'l2vpn-svc:bw-per-svc')" {
              description
                "Relevant when the bandwidth type is
                 set as bandwidth per VPN service.";
            }
            type svc-id;
            description
              "Identifies the target VPN.  If the bandwidth
               type is set as bandwidth per VPN service, the
               vpn-id MUST be specified.";
          }
          leaf cir {
            type uint64;
            units "bps";
            mandatory true;
            description
              "Committed Information Rate.  The maximum number
               of bits that a port can receive or send over
               an interface in one second.";
          }
          leaf cbs {
            type uint64;
            units "bps";
            mandatory true;
            description
              "Committed Burst Size (CBS).  Controls the bursty
               nature of the traffic.  Traffic that does not
               use the configured Committed Information Rate
               (CIR) accumulates credits until the credits
```

```
                reach the configured CBS.";
            }
            leaf eir {
              type uint64;
              units "bps";
              description
                "Excess Information Rate (EIR), i.e., excess frame
                 delivery allowed that is not subject to an SLA.
                 The traffic rate can be limited by the EIR.";
            }
            leaf ebs {
              type uint64;
              units "bps";
              description
                "Excess Burst Size (EBS).  The bandwidth available
                 for burst traffic from the EBS is subject to the
                 amount of bandwidth that is accumulated during
                 periods when traffic allocated by the EIR
                 policy is not used.";
            }
            leaf pir {
              type uint64;
              units "bps";
              description
                "Peak Information Rate, i.e., maximum frame
                 delivery allowed.  It is equal to or less
                 than the sum of the CIR and the EIR.";
            }
            leaf pbs {
              type uint64;
              units "bps";
              description
                "Peak Burst Size.  It is measured in bytes per
                 second.";
            }
            description
              "List of bandwidth values (e.g., per CoS,
               per vpn-id).";
          }
          description
            "From the customer site's perspective, the service
             input/output bandwidth of the connection or
             download/upload bandwidth from the SP/site
             to the site/SP.";
        }
        leaf svc-mtu {
          type uint16;
          units "bytes";
          mandatory true;
          description
            "SVC MTU.  It is also known as the maximum
             transmission unit or maximum frame size.  When
             a frame is larger than the MTU, it is broken
             down, or fragmented, into smaller pieces by
             the network protocol to accommodate the MTU
             of the network.  If CsC is enabled,
             the requested svc-mtu leaf will refer to the
             MPLS MTU and not to the link MTU.";
        }
        uses site-service-qos-profile;
        uses site-service-mpls;
        description
          "Container for services.";
      }
      uses site-bum;
      uses site-mac-loop-prevention;
      uses site-acl;
      container mac-addr-limit {
        if-feature "mac-addr-limit";
        leaf limit-number {
          type uint16;
          default "2";
          description
            "Maximum number of MAC addresses learned from
             the subscriber for a single service instance.
             The default allowed maximum number of MAC
             addresses is 2.";
        }
        leaf time-interval {
          type uint32;
          units "seconds";
          default "300";
          description
            "The aging time of the MAC address.  By default,
             the aging time is set to 300 seconds.";
        }
```

```
              leaf action {
                type identityref {
                  base mac-action;
                }
                default "warning";
                description
                  "Specifies the action taken when the upper limit is
                   exceeded: drop the packet, flood the packet, or
                   simply send a warning log message.  By default,
                   the action is set to 'warning'.";
              }
              description
                "Container of MAC address limit configurations.";
            }
            description
              "List of site network accesses.";
          }
          description
            "Container of port configurations.";
        }
        description
          "List of sites.";
      }
      description
        "Container of site configurations.";
    }
    description
      "Container for L2VPN services.";
  }
}

<CODE ENDS>
```

9. Вопросы безопасности

Модуль YANG, заданный в этом документе, определяет схему данных, которые предназначены для доступа по протоколам сетевого управления, таким как NETCONF [RFC6241] или RESTCONF [RFC8040]. Нижним уровнем NETCONF является защищённый транспорт, а обязательным для реализации транспортом - SSH[1] [RFC6242]. Нижним уровнем протокола RESTCONF является HTTPS и обязательна реализация защищённого транспорта TLS [RFC8446].

Модель управления доступом NETCONF [RFC8341] обеспечивает способы ограничения доступа, разрешая его конкретным пользователям NETCONF или RESTCONF к заранее заданному набору всех доступных операций протокола NETCONF или RESTCONF, а также компонентам содержимого.

В этом модуле YANG определено множество узлов данных, которые разрешают запись/изменение/удаление (т. е. используют принятое по умолчанию значение config true). Эти узлы данных могут быть уязвимыми или конфиденциальными в некоторых средах. Операции записи (например, edit-config) в такие узлы без подобающей защиты могут оказывать негативное влияние на работу сети. Ниже перечислены такие субдеревья и узлы данных.

- **/l2vpn-svc/vpn-services/vpn-service**

  Записи в этом списке включают все конфигурации сервиса VPN, на которые абонент подписан и будет применять для непрямого создания или изменения конфигурации устройств PE и CE. Неожиданные изменения этих записей могут вести к нарушению сервиса и/или недопустимому поведению сети.

- **/l2vpn-svc/sites/site**

  Записи этого списка включают конфигурации абонентского сайта. Неожиданные изменения этих записей могут вести к нарушению сервиса и/или недопустимому поведению сети.

Некоторые из доступных для чтения узлов данных в этом модуле YANG могут быть уязвимыми или конфиденциальными в отдельных сетевых средах. Важно контролировать доступ (например, get, get-config, notification) к таким узлам. Ниже перечислены такие субдеревья и узлы данных.

- **/l2vpn-svc/vpn-services/vpn-service**
- **/l2vpn-svc/sites/site**

Записи в указанных выше списках содержат приватную или конфиденциальную информацию, например, название абонента, местоположение сайта, услуги, на которые подписан абонент.

При взаимодействии SP с множеством абонентов важно обеспечить, чтобы каждый абонент мог видеть и менять лишь информацию о своих услугах.

Модель данных определяет некоторые параметры защиты, которые могут быть расширены с помощью дополнений. Эти параметры описаны в параграфах 5.12 и 5.13.

10. Взаимодействие с IANA

Агентство IANA выделило новое значение URI в реестре «IETF XML Registry» [RFC3688].

```
URI: urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc
Registrant Contact: The IESG
XML: N/A; the requested URI is an XML namespace
```

Агентство IANA выделило новое имя модуля YANG в реестре «YANG Module Names» [RFC6020].

[1]Secure Shell.

```
name: ietf-l2vpn-svc
namespace: urn:ietf:params:xml:ns:yang:ietf-l2vpn-svc
prefix: l2vpn-svc
reference: RFC 8466
```

11. Литература

11.1. 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>.

[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>.

[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>.

[RFC6073] Martini, L., Metz, C., Nadeau, T., Bocci, M., and M. Aissaoui, "Segmented Pseudowire", RFC 6073, DOI 10.17487/RFC6073, January 2011, <https://www.rfc-editor.org/info/rfc6073>.

[RFC6074] Rosen, E., Davie, B., Radoaca, V., and W. Luo, "Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)", RFC 6074, DOI 10.17487/RFC6074, January 2011, <https://www.rfc-editor.org/info/rfc6074>.

[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>.

[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>.

[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>.

[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>.

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

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

[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>.

[W3C.REC-xml-20081126] Bray, T., Paoli, J., Sperberg-McQueen, M., Maler, E., and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <https://www.w3.org/TR/2008/REC-xml-20081126>.

11.2. Дополнительная литература

[EVPN-YANG] Brissette, P., Ed., Shah, H., Ed., Chen, I., Ed., Hussain, I., Ed., Tiruveedhula, K., Ed., and J. Rabadan, Ed., "Yang Data Model for EVPN", Work in Progress, draft-ietf-bess-evpn-yang-05, February 2018.

[IEEE-802-1ag] IEEE, "802.1ag - 2007 - IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management", DOI 10.1109/IEEESTD.2007.4431836.

[IEEE-802-1D] IEEE, "802.1D-2004 - IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges", DOI 10.1109/IEEESTD.2004.94569.

[IEEE-802-1Q] IEEE, "802.1Q - 2014 - IEEE Standard for Local and metropolitan area networks--Bridges and Bridged Networks", DOI 10.1109/IEEESTD.2014.6991462.

[IEEE-802-3ah] IEEE, "802.3ah - 2004 - IEEE Standard for Information technology-- Local and metropolitan area networks-- Part 3: CSMA/CD Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks", DOI 10.1109/IEEESTD.2004.94617.

[ITU-T-Y-1731] International Telecommunication Union, "Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks", ITU-T Recommendation Y.1731, August 2015, <https://www.itu.int/rec/T-REC-Y.1731/en>.

[MEF-6] Metro Ethernet Forum, "Ethernet Services Definitions - Phase 2", April 2008, <https://mef.net/PDF_Documents/technical-specifications/MEF6-1.pdf>.

[MPLS-L2VPN-YANG] Shah, H., Ed., Brissette, P., Ed., Chen, I., Ed., Hussain, I., Ed., Wen, B., Ed., and K. Tiruveedhula, Ed., "YANG Data Model for MPLS-based L2VPN", Work in Progress, draft-ietf-bess-l2vpn-yang-08, February 2018.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, DOI 10.17487/RFC4119, December 2005, <https://www.rfc-editor.org/info/rfc4119>.

[RFC6624] Kompella, K., Kothari, B., and R. Cherukuri, "Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling", RFC 6624, DOI 10.17487/RFC6624, May 2012, <https://www.rfc-editor.org/info/rfc6624>.

[RFC7130] Bhatia, M., Ed., Chen, M., Ed., Boutros, S., Ed., Binderberger, M., Ed., and J. Haas, Ed., "Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces", RFC 7130, DOI 10.17487/RFC7130, February 2014, <https://www.rfc-editor.org/info/rfc7130>.

[RFC7209] Sajassi, A., Aggarwal, R., Uttaro, J., Bitar, N., Henderickx, W., and A. Isaac, "Requirements for Ethernet VPN (EVPN)", RFC 7209, DOI 10.17487/RFC7209, May 2014, <https://www.rfc-editor.org/info/rfc7209>.

[RFC7348] Mahalingam, M., Dutt, D., Duda, K., Agarwal, P., Kreeger, L., Sridhar, T., Bursell, M., and C. Wright, "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks", RFC 7348, DOI 10.17487/RFC7348, August 2014, <https://www.rfc-editor.org/info/rfc7348>.

[RFC7436] Shah, H., Rosen, E., Le Faucheur, F., and G. Heron, "IP-Only LAN Service (IPLS)", RFC 7436, DOI 10.17487/RFC7436, January 2015, <https://www.rfc-editor.org/info/rfc7436>.

[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>.

[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>.

Благодарности

Спасибо Qin Wu и Adrian Farrel за содействие в работе над предварительными версиями документа. Спасибо Zonghe Huang, Wei Deng и Xiaoling Song за рецензирование этого документа.

Отдельная благодарность Jan Lindblad за внимательное рецензирование YANG.

Этот документ основан на работе группы L3SM, представленной в [RFC8299].

Адреса авторов

Bin Wen
Comcast
Email: bin_wen@comcast.com

Giuseppe Fioccola (редактор)
Telecom Italia
Email: giuseppe.fioccola@tim.it

Chongfeng Xie
China Telecom
Email: xiechf.bri@chinatelecom.cn

Luay Jalil
Verizon
Email: luay.jalil@verizon.com

Перевод на русский язык
Николай Малых

nmalykh@protokols.ru