Программируемые Сети ООО
117342, г. Москва, ул. Бутлерова, д.17

+7 (499) 649 46 46
www.Brain4Net.ru
need@brain4net.com

РУКОВОДСТВО ПО ПЛАНИРОВАНИЮ И ВНЕДРЕНИЮ

B4N SD-WAN

Версия 2.20.12

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
1. ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ, ТЕРМИНОВ И СОКРАЩЕНИЙ 5
2. НАЗНАЧЕНИЕ 10
3. АРХИТЕКТУРА И СОСТАВ РЕШЕНИЯ B4N SD-WAN 12
3.1. Архитектура B4N SD-WAN 12
3.2. Компоненты B4N SD-WAN 14
3.3. Автоматическая настройка CPE 15
4. РАЗВЕРТЫВАНИЕ СЕРВИСА B4N SD-WAN 18
4.1. VNF SD-WAN и шаблон сетевого сервиса SD-WAN 18
4.2. PNF SD-WAN 19
4.3. Шаблон инстанса SD-WAN (SD-WAN Instance template) 20
4.4. Шаблон CPE 22
4.4.1. Типы CPE 22
4.4.2. Назначение и разделы шаблона CPE 23
4.4.3. Операции с шаблонами CPE 24
4.4.3.1. Экспорт и импорт шаблонов CPE 25
4.4.3.2. Клонирование шаблонов CPE 25
4.5. Создание тенанта 25
4.6. Развертывание сервиса SD-WAN для тенанта 26
4.7. Регистрация CPE 26
5. ИНВЕНТАРИЗАЦИОННАЯ БАЗА CPE 28
5.1. Добавление CPE в инвентаризационную базу 28
5.2. Действия с CPE 30
6. СОСТАВ И ОПИСАНИЕ SD-WAN GATEWAY И SD-WAN CPE 32
6.1. Описание SD-WAN шлюзов 32
6.2. Описание CPE 33
6.3. Описание uCPE 34
7. УПРАВЛЕНИЕ И МОНИТОРИНГ CPE 36
7.1. Управление CPE 36
7.2. Мониторинг CPE 37
7.3. Локальная диагностика CPE 37
8. УПРАВЛЕНИЕ ТРАФИКОМ 39
8.1. Использование нескольких путей для передачи трафика 39

8.2. Создание сервисов с SLA 40
8.3. Фильтрация трафика 44
8.3.1. Создание правил классификации трафика 45
8.3.2. Создание фильтров трафика 46
8.4. Маршрутизация трафика по приложениям 47
9. РЕЗЕРВИРОВАНИЕ И ОТКАЗОУСТОЙЧИВОСТЬ 50
9.1. Резервирование центральных компонентов 50
9.2. Резервирование каналов связи с CPE 53
9.3. Link Dampening 55
10. ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ 56
10.1. Требования к аппаратному обеспечению 56
10.2. Требования к программному обеспечению 57
10.3. Требования к CPE 58
11. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ 60
11.1. Аутентификация и авторизация 60
11.2. Использование безопасных протоколов управления 61
11.3. Безопасное подключение CPE и контроль конфигурации 62
11.4. Использование VNF с функциональностью защиты данных 62
12. СЦЕНАРИИ ПРИМЕНЕНИЯ 62
12.1. Организация топологии Hub-and-Spoke без возможности связи между удаленными офисами 63
12.2. Организация топологии Hub-and-Spoke с возможностью связи между офисами через центральный офис 63
12.3. Организация топологии Hub-and-Spoke с возможностью связи между офисами через сервисную цепочку в ЦОД 64
12.4. Организация услуги L3 VPN 65
13. ЗАКЛЮЧЕНИЕ 66

ВВЕДЕНИЕ

SD-WAN (Software Defined WAN) — программно-определяемые распределенные сети — это технология распределения сетевого трафика по каналам сети передачи данных, использующая концепцию SDN (Software Defined Networking) для автоматического определения наиболее эффективных путей маршрутизации трафика.

Основным принципом SDN является разделение функционала управления сетью (Control Plane) и функционала коммутации пакетов (Data Plane). Централизация функций контроля сети делает возможным программирование сетей с помощью открытых API, автоматизацию процессов и оркестрацию сервисов.

В соответствии с концепцией SDN, в технологии SD-WAN весь интеллект, связанный с логикой управления распределенной сетью, переносится в центр. SD-WAN контроллер отвечает за управление абонентскими устройствами (CPE - Customer Premises Equipment). Контроллер взаимодействует, с одной стороны, с оркестратором, который используется для верхнеуровневого управления сетью и имеет API для управления сервисами, и с другой стороны, с устройствами CPE, которые образуют уровень коммутации данных (forwarding plane).

В традиционных распределенных сетях настройка сети происходит последовательно, устройство за устройством, функция за функцией: например, определяются классы QoS, политики, правила маршрутизации, функции безопасности. Эти действия выполняются квалифицированными инженерами, тем не менее существует вероятность ошибки. Технология SD-WAN позволяет избежать ручных настроек, и в то же время обеспечивает интеллектуальное управление трафиком в реальном времени и автоматическое реагирование на изменение топологии сети.

Решение SD-WAN предназначено для замены традиционных маршрутизаторов в распределенных сетях и не зависит от используемых транспортных технологий.

1. ПЕРЕЧЕНЬ УСЛОВНЫХ ОБОЗНАЧЕНИЙ, ТЕРМИНОВ И СОКРАЩЕНИЙ

Сокращение	Расшифровка
Администратор тенанта	Функциональная роль по управлению логически обособленной частью ресурсов - тенантом.
Виртуальная машина (ВМ)	Полностью изолированный программный контейнер (модуль), работающий с собственной операционной системой и приложениями, аналогично физическому серверу. ВМ обладает собственными: – процессорными ресурсами, – местом на жестком диске, – оперативной памятью, – операционной системой.
Виртуальный ЦОД	Сервис аренды вычислительных мощностей для создания собственной инфраструктуры в «облаке». Характеризуется следующими параметрами: – Суммарная вычислительная мощность процессоров – Оперативная память – Дисковое пространство: объем и скорость – IP-сети: количество и размер, количество внешних IP адресов – Максимальное количество виртуальных машин
Домен	Множество элементов инфраструктуры, объединенных единой системой политик, предназначенных для реализации определенного функционала.
ЦОД	Центр обработки данных (Data Center) – специализированная технологическая площадка, предназначенная для размещения серверного и коммуникационного оборудования.
ARM архитектура	Архитектура ARM (Advanced RISC Machine) — усовершенствованная RISC-машина — семейство лицензируемых 32-битных и 64-битных микропроцессорных ядер разработки компании ARM Limited.
CP	Connnection Point - Точка подключения пользователя к сетевому домену, без привязки к какому-либо сервису. Имеет разные типы инкапсуляции (Access, VLAN, QinQ и т.д.)
CPE	Customer Premises Equipment - телекоммуникационное оборудование, расположенное в помещении абонента/клиента. Оборудование обычно используется для соединения абонента/клиента с публичной или частной сетью оператора связи.
DC	Логическая сущность, представляющая агрегацию сетевых и вычислительных ресурсов (Data Center, Telco PoP). Всегда вложена в Infrastructure Domain.
DPDK	Data Plane Development Kit - набор библиотек и драйверов для быстрой обработки сетевых пакетов в приложениях, работающих на архитектуре Intel.

E-LAN	То же самое, что и M2M service
E-Line	То же самое, что и P2P service
E-Tree	То же самое, что и P2M service
EVC	Ethernet virtual circuits - виртуальное соединение Ethernet - соединение двух или более пользовательских сетевых интерфейсов на втором уровне (данные передаются в виде Ethernet фреймов).
IaaS	Инфраструктура как услуга (Infrastructure as a service) – бизнес-модель обеспечения и использования виртуальной и аппаратной ИТ-инфраструктуры, при которой вычислительные мощности ЦОД предоставляются абонентам во временное пользование.
IGMP	Internet Group Management Protocol — протокол управления групповой (multicast) передачей данных в сетях, основанных на протоколе IP.
Infrastructure Domain	Инфраструктурный домен - Логическая сущность для группировки нескольких ЦОД (DC), SDN контроллеров.
KVM	Kernel-based Virtual Machine — программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86.
L3VPN	Сервис контроллера, представляющий собой логический маршрутизатор между двумя или более L3-SI
M2M-service	Соединение типа «каждый с каждым». Например, соединение всех офисов в единую сеть, где каждый филиал может общаться с другими через логические туннели.
MPLS	Multiprotocol label switching — многопротокольная коммутация по меткам) — механизм в телекоммуникационной сети, осуществляющий передачу данных от одного узла сети к другому с помощью меток.
NaaS	Сеть как сервис (Network as a Service) – предоставление сетевых услуг конечным пользователям на инфраструктуре провайдера с применением единого процесса заказа и обеспечением стандартных процессов обслуживания.
NAT	Network Address Translation - механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.
NFV	Network Function Virtualization – виртуализация сетевых функций или реализация сетевых функций на виртуальной инфраструктуре.
NFVI	Network Function Virtualization Infrastructure – инфраструктура для обеспечения функционирования приложений NFV.

NFVO	NFV Orchestrator – Оркестратор виртуализации сетевых функций
NNI	Network-to-network interface - Интерфейс в сторону другого узла сети.
NS (Network Service)	Сетевой сервис, набор виртуальных сетевых функций и соединений между ними.
OF-port	Логический порт коммутатора, который организуется Openflow-агентом и через который контроллер взаимодействует с коммутатором по протоколу OpenFlow. Openflow-контроллер оперирует OF-портами коммутатора, для него Interface = OF-port.
Orchestrator	Система управления NFV / SDN-платформой
OSS	Домен систем эксплуатации и поддержки операций (Operation Support System) – набор корпоративных информационных систем, предназначенных для автоматизации процессов взаимодействия управляющего персонала, сервисов и элементов инфраструктуры.
OSS / BSS	Operation Support System / Billing Support System - Системы для управления услугами с точки зрения бизнеса
P2M-service	Соединение типа «все с одним». Например, соединение всех филиалов с центральным офисом, при котором филиалы не имеют возможности общаться между собой напрямую.
P2P-service	Туннель от одной точки до другой.
PCP	Priority code point - поле длиной 3 бита в заголовке 802.1Q, которое в соответствии со стандартом IEEE 802.1p определяет класс обслуживания трафика и влияет на приоритет его обработки.
PNF	Physical Network Function - физические сетевые функции - отдельно стоящие аппаратные сетевые устройства, либо отдельно стоящие виртуальные машины, развернутые не оркестратором.
SI	Service Interface - Сервисный интерфейс пользователя к конкретному сервису. Представляет собой CP, включенный в состав какого-либо сервиса.
QinQ	QinQ (IEEE 802.1QinQ) — расширение к стандарту IEEE 802.1Q, описывающее как тегированный трафик может передаваться внутри уже тегированного по 802.1Q трафика.

QoS (Quality of service)	Гарантированное качество сервиса.
RBAC	Role-based access control - контроль доступа пользователей к системе на основе ролей
SDN	Software-Defined Networking - программно-конфигурируемая сеть - сеть передачи данных, в которой уровень управления сетью отделён от устройств передачи данных и реализуется в виде программного обеспечения.
SDN контроллер	Базовый элемент сетевой инфраструктуры SDN - центральное управляющее устройство, осуществляющее контроль и программирование связанных между собой коммутаторов по какому-либо протоколу управления.
SD-WAN	Software Defined networking in a wide area network (WAN).
SLA (Service level agreement)	Соглашение между заказчиком и его поставщиком о параметрах и уровне качества сервиса
Tenant (Pool / Network Slice)	Логический пул ресурсов, выделенный клиенту или под конкретные задачи оператора. Тенант может объединять в себе ресурсы нескольких ЦОД, доменов и т. д. Например, если офисы клиента разнесены по разным городам страны, то в каждом городе ему могут быть выделены вычислительные и сетевые ресурсы, которые все вместе образуют один тенант.
UNI	User Network Interface (интерфейс подключения пользователя) - физический интерфейс/точка разграничения ответственности между сервис-провайдером и клиентом.
vCPE	Virtual Customer Premises Equipment - виртуализация абонентских сетевых устройств/сервисов.
VDU	Virtual Deployment Unit - Виртуальная машина/ы в составе VNF.
VIM (Virtualized Infrastructure Manager)	Менеджер виртуальной инфраструктуры, ПО, отвечающее за конфигурацию и управление виртуальной инфраструктурой. В данный момент наиболее популярные VIM — это OpenStack и VMware vSphere vCenter.
VL (virtual links)	Связь любого типа между устройствами. Примеры: P2P, M2M и т. д.
VLAN	Virtual Local Area Network - виртуальная локальная сеть.
VM	Виртуальная машина.

VNF (Virtual Network Function)	Виртуальная сетевая функция. Пользователи применяют эти функции для создания виртуальной сетевой инфраструктуры. Сетевые функции представлены в каталоге. VNF могут быть простыми (состоящими из одной функции) или комплексными (состоящими из нескольких объединенных в группу виртуальных сетевых функций).
VNFD	Дескриптор, описывающий VNF.
VNFM	Менеджер виртуальных сетевых функций.
VNF Package	Пакет, содержащий образы VDU, VNFD, конфигурационные скрипты.
VXLAN	Virtual Extensible LAN - технология сетевой виртуализации, созданная для решения проблем масштабируемости в больших системах облачных вычислений. Использует инкапсуляцию Layer 2 Ethernet кадров в UDP-пакеты.

2. НАЗНАЧЕНИЕ

Решение B4N SD-WAN входит в состав платформы B4N Service Platform – комплексного решения для модернизации сетевой инфраструктуры операторов связи, центров обработки данных и распределенных корпоративных сетей на базе технологий SDN и NFV. Платформа включает в себя компоненты для оркестрации сетевых сервисов, организации высокоскоростной обработки трафика и виртуализации сетевых функций.

Решение B4N SD-WAN предназначено в первую очередь для операторов связи и компаний, имеющих крупную филиальную сеть. B4N Service Platform является мультитенантной платформой, позволяя предоставлять сервис SD-WAN множеству независимых организаций, являющихся клиентами сервис провайдера, или подразделениям одного предприятия.

Основные задачи B4N SD-WAN:

- Интеллектуальное управление трафиком
- Автоматическая настройка устройств, устанавливаемых на сайтах заказчиков (CPE - Customer Premises Equipment)
- Централизованное управление инфраструктурой
- Мониторинг и автоматическое реагирование на изменение топологии сети и требований приложений к качеству обслуживания
- Возможность для Заказчиков динамически управлять услугой через портал самообслуживания.

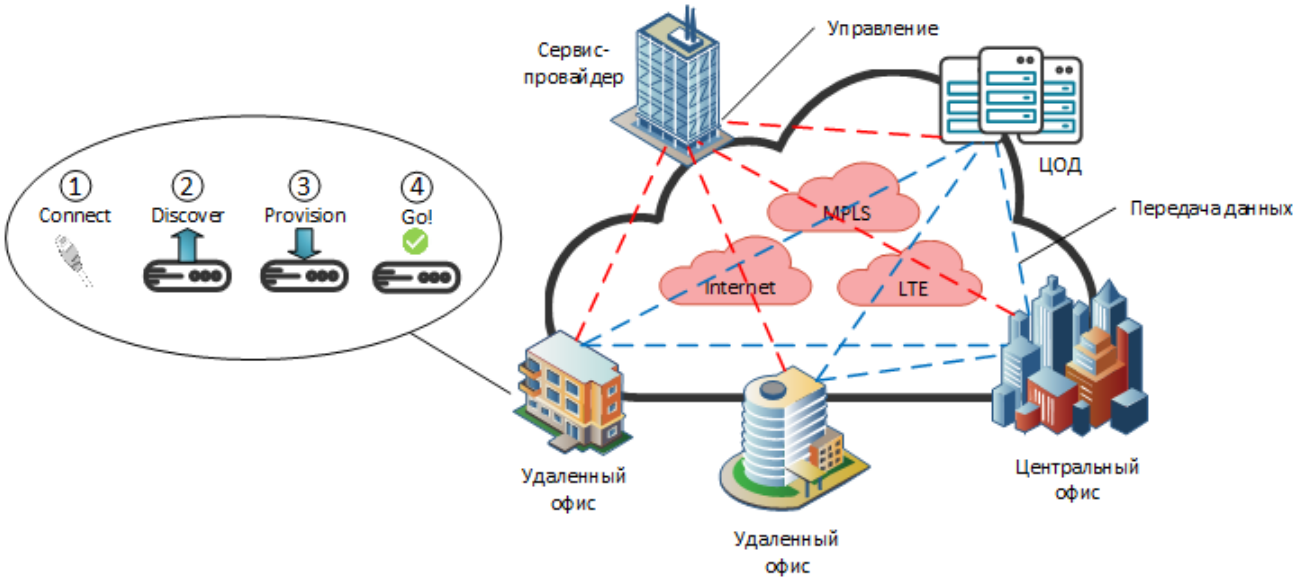

Рис. 1. Концепция SD-WAN

Концепция SD-WAN предполагает создание виртуальных каналов (туннелей) поверх существующих транспортных сетей, в качестве которых могут использоваться сервисы MPLS, широкополосные каналы для подключения к Интернет, арендуемые линии связи, беспроводные подключения, в том числе LTE (Рис. 1). Обычно создается несколько туннелей, и все они используются для передачи трафика с учетом требований приложений к пропускной способности и качеству обслуживания.

Характеристики решения B4N SD-WAN:

- Независимость от используемых физических сетей связи (underlay), способность работать поверх проводных и беспроводных сетей доступа любого типа;

- Постоянный мониторинг каждого туннеля SD-WAN с целью автоматического переключения на резервный маршрут в случае сбоя канала связи;
- Обеспечение высокой доступности путем одновременного использования нескольких WAN-каналов;
- Централизованное управление, контроль и оркестрация туннелей SD-WAN, автоматическая настройка устройств, устанавливаемых на сайтах заказчиков.

Решение B4N SD-WAN учитывает основные требования сервис-провайдеров к устройствам, устанавливаемым на площадках Заказчиков:

- Стандартная архитектура x86 или ARM. Отсутствие зависимости от определенных производителей оборудования даже для младших моделей CPE.
- Минимальные требования к аппаратным ресурсам (процессору, оперативной памяти) и, соответственно, низкая цена устройств.

Поддерживаются CPE двух типов:

1. CPE, выполняющие только транспортную функцию;
2. Universal CPE (uCPE) - устройства, на которых дополнительно могут запускаться виртуальные сетевые функции (VNF).

Роль CPE 1-го типа сводится к доставке трафика из офиса Заказчика в ЦОД сервис-провайдера (Рис. 2). Сетевые функции, которые обычно выполнялись на устройствах, установленных на площадках Заказчика (работа протоколов маршрутизации, NAT, защита сети и т.п.) могут быть предоставлены из облака провайдера. Для этого решение SD-WAN должно быть тесно интегрировано с решением vCPE (virtual CPE), то есть должна быть возможность маршрутизировать трафик от CPE в соответствующую сервисную цепочку в ЦОД оператора, включающую в себя одну или несколько виртуальных сетевых функций (например, виртуальный маршрутизатор, межсетевой экран, система предотвращения вторжений, антивирус и т.п.) перед передачей к месту назначения.

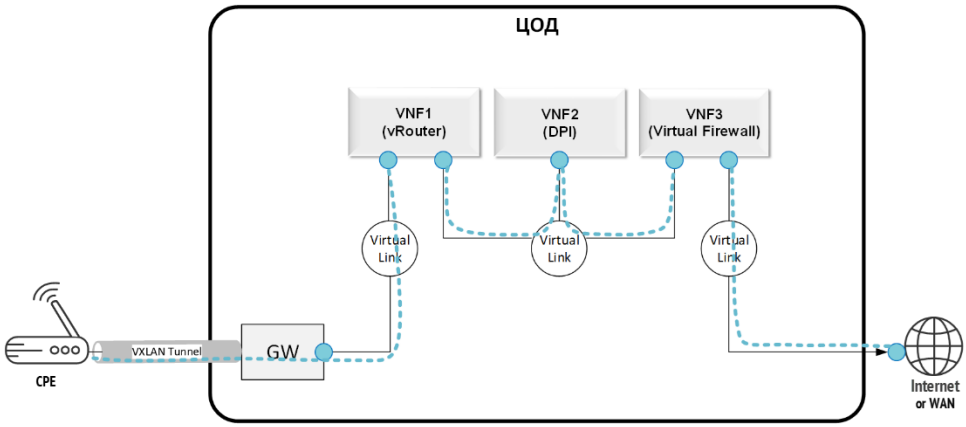

Рис. 2. Передача трафика от CPE в сервисную цепочку в ЦОД

CPE 2-го типа (uCPE) должны иметь достаточно ресурсов, чтобы обеспечить развертывание одной или нескольких VNF непосредственно на самом устройстве, не используя ресурсы облака. На рисунке 3 представлен отказоустойчивый вариант с установкой двух uCPE на удаленной площадке. Локальное размещение функций улучшает время отклика и оптимизирует транспортные потоки. При этом CPE и виртуальные функции, развернутые на них, остаются под управлением централизованного оркестратора.

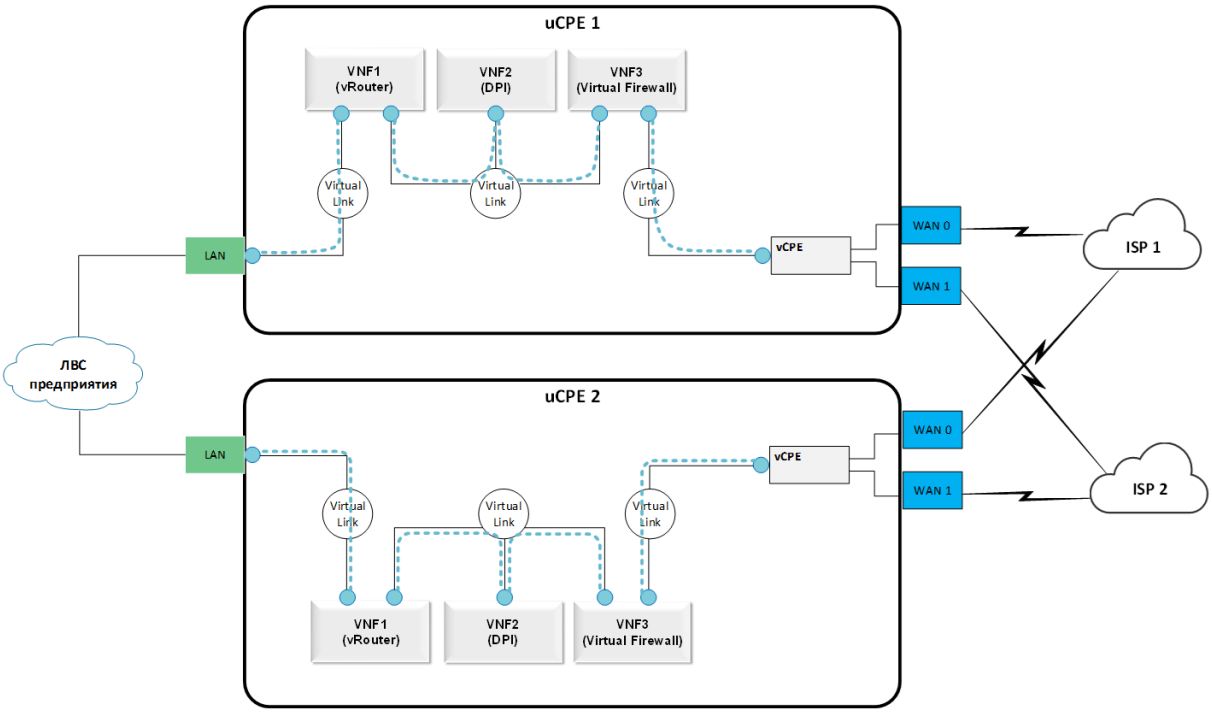

Рис. 3. Развертывание сервисной цепочки на uCPE

3. АРХИТЕКТУРА И СОСТАВ РЕШЕНИЯ B4N SD-WAN

3.1. Архитектура B4N SD-WAN

Основными функциональными элементами решения B4N SD-WAN являются B4N оркестратор, SD-WAN контроллер, SD-WAN шлюзы, CPE (Рис. 4). Устройства CPE размещаются на сайтах заказчиков, остальные элементы разворачиваются в ЦОД.

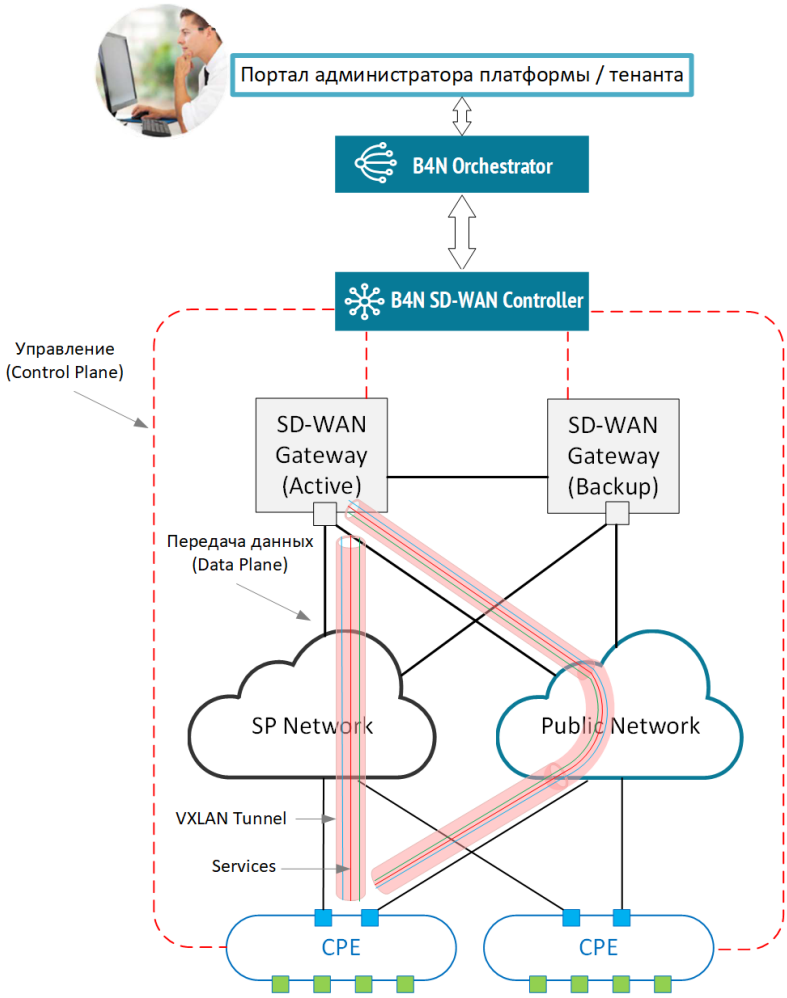

Рис. 4. Верхнеуровневая архитектура B4N SD-WAN

Оркестратор содержит графический пользовательский портал, с помощью которого администратор сети управляет сервисом SD-WAN и абонентскими устройствами.

CPE подключаются к SD-WAN шлюзам с помощью туннелей VXLAN, образуя SDN-фабрику в виде наложенной сети (overlay).

SD-WAN шлюзы являются обязательным элементом сети и служат для объединения CPE в единую сеть. На SD-WAN шлюзах терминируются VXLAN туннели, и трафик передается далее в соответствии с топологией сервиса. В целях отказоустойчивости SD-WAN шлюзы всегда устанавливаются парами.

SD-WAN контроллер отвечает за управление наложенной сетью - построение актуальной топологии, создание транспортных сервисов внутри VXLAN туннелей (L2 Point-to-Point, Point-to-Multipoint, Multipoint-to-Multipoint, l3 VPN). С точки зрения SD-WAN Контроллера абонентские устройства CPE и SD-WAN шлюзы являются SDN-коммутаторами, управляемыми по протоколу OpenFlow.

Оркестратор может управлять несколькими сервисами SD-WAN, созданными, например, для разных заказчиков или регионов. Каждый сервис SD-WAN имеет собственный кластер SD-WAN контроллеров и SD-WAN шлюзы.

SD-WAN контроллер и SD-WAN шлюзы разворачиваются в системе в виде виртуальной сетевой функции (VNF) или отдельных виртуальных машин. В последнем случае они добавляются в оркестратор как PNF (Physical

Network Function). Использование PNF позволяет исключить необходимость в менеджере виртуальной инфраструктуры (VIM) в ЦОД.

Для каждого тенанта (клиента оператора связи или подразделения крупной компании) создается собственный сервис SD-WAN. Это позволяет обеспечить полную независимость распределенных сетей разных организаций друг от друга.

Возможен сценарий, когда требуется создать общую сеть SD-WAN для нескольких небольших компаний с малым количеством CPE. В этом случае имеется возможность создать один транспортный тенант, внутри которого создаются клиентские тенанты. SD-WAN контроллер и шдюзы для этих клиентских тенантов будут общими, но CPE, сетевые сервисы и портал самообслуживания у каждого тенанта будут свои.

3.2. Компоненты B4N SD-WAN

Обязательными компонентами при развертывании решения B4N SD-WAN являются:

- B4N оркестратор;
- VNFM — отвечает за конфигурацию VNF и CPE;
- SD-WAN контроллер;
- SD-WAN шлюзы.

Если сервис SD-WAN развертывается с использованием VNF SD-WAN, то дополнительно в состав решения входят компоненты:

- DC Controller — SDN-контроллер, управляющий виртуальными коммутаторами и отвечающий за создание виртуальных линков между VNF в ЦОД;
- VIM — менеджер виртуальной инфраструктуры.

Перед развертыванием сервиса SD-WAN в портале управления оркестратора создается тенант - логический пул ресурсов. В рамках тенанта запускается специализированный сетевой сервис SD-WAN Network Service (NS), основным элементом которого является VNF или PNF SD-WAN, включающие в себя:

- SD-WAN Controller - SDN-контроллер, который прописывает правила OpenFlow на CPE и SD-WAN шлюзах в рамках одного тенанта. Отвечает за распределение трафика между туннелями, мониторинг качества соединения и автоматическое переключение трафика на резервный туннель в случае возникновения проблем на основном;
- SD-WAN шлюзы - программные коммутаторы OpenFlow, на которых терминируются VXLAN туннели, инициированные от CPE.

CPE и SD-WAN NS могут являться частью сервисной цепочки с включением других VNF, развернутых в ЦОД.

Взаимосвязи между компонентами решения приведены на рисунке 5. SD-WAN контроллер может состоять из одного узла или развертываться в виде кластера из трех узлов. Узлы кластера SD-WAN контроллера и шлюзы представляют собой отдельные виртуальные машины (VDU) и могут быть запущены на разных аппаратных серверах в целях обеспечения отказоустойчивости.

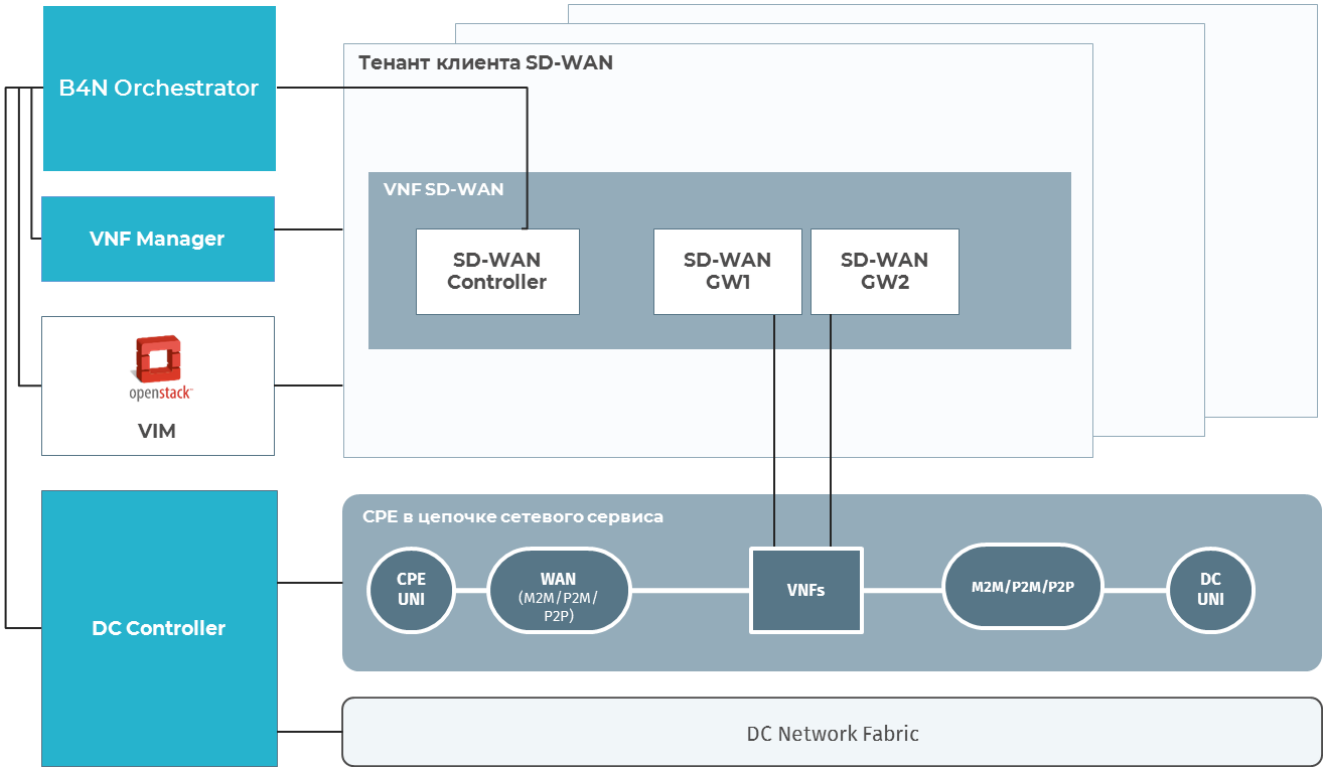

Рис. 5. Основные компоненты сервиса SD-WAN

CPE UNI и DC UNI - это сервисные интерфейсы точек подключения сервисной цепочки к локальной сети ЦОД.

3.3. Автоматическая настройка CPE

Каждое устройство CPE имеет уникальный идентификатор DPID (Datapath Identifier). Это 64-битное число, генерируемое на основе уникальной для данного устройства характеристики оборудования, например, MAC адреса интерфейса WAN0, серийного номера или другого идентификатора.

Перед отправкой на площадку заказчика CPE добавляется в инвентаризационную базу оркестратора (CPE Inventory) с указанием DPID и “привязкой” к тенанту.

Далее подключение к SD-WAN контроллеру и автоматическая настройка CPE (zero touch provisioning) осуществляются следующим образом (Рис. 6):

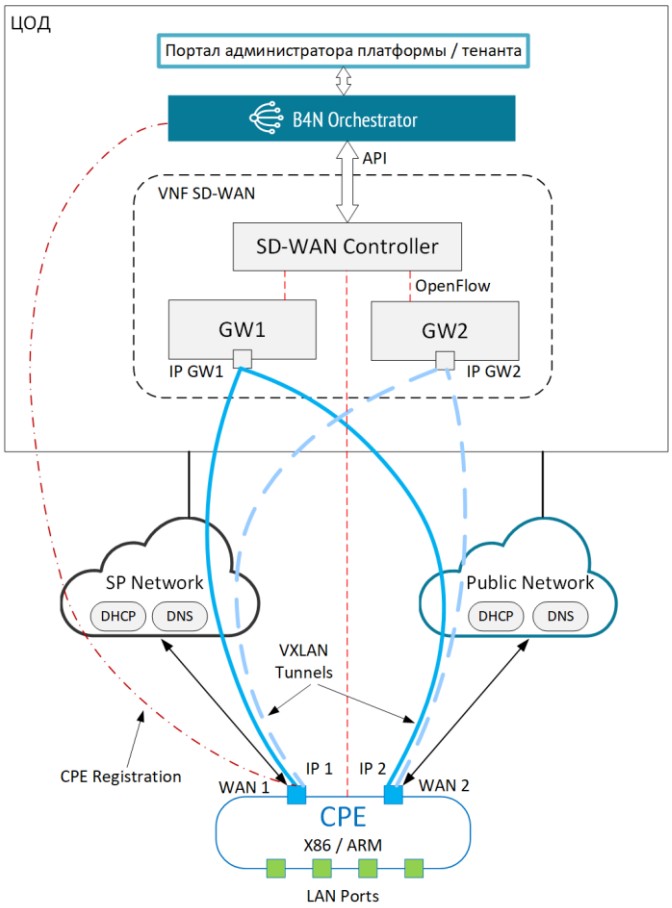

Рис. 6. Подключение CPE

1. CPE получает внешние IP адреса для портов WAN, маршруты по умолчанию и IP адреса серверов DNS от операторов связи по DHCP.
2. Используя преднастроенное доменное имя B4N оркестратора (FQDN), CPE связывается с ним, сообщает свой идентификатор (DPID) и получает внешние IP адреса SD-WAN контроллера и шлюзов.
3. CPE устанавливает служебное соединение с SD-WAN контроллером по протоколу TLS через IP сеть (сеть оператора или Интернет).
4. SD-WAN контроллер посылает команды на CPE для создания VXLAN туннелей с каждого WAN-порта к каждому SD-WAN шлюзу в составе сервиса SD-WAN для данного тенанта.
5. SD-WAN контроллер программирует CPE и SD-WAN шлюзы с целью создания транспортных SDN-сервисов требуемой топологии.

Для автоматической настройки CPE через Интернет необходимо, чтобы у оркестратора, SD-WAN-контроллера и SD-WAN шлюзов были настроены внешние (public) IP адреса.

Если выделить отдельные внешние IP адреса нет возможности, может быть настроен статический NAT для следующих портов:

- Для оркестратора - порт tcp 443, 81
- Для SD-WAN контроллера - порт tcp 6653
- Для SD-WAN шлюзов - порты udp 4800 – 4819 (значения и количество udp портов зависит от количества WAN-интерфейсов на CPE).

CPE могут находиться за NAT.

Если устройство CPE предварительно не было внесено в инвентаризационную базу, но пытается зарегистрироваться в оркестраторе, оно будет отображаться в CPE Inventory со статусом Unknown. Администратор может удалить его или зарегистрировать, указав, какому тенанту принадлежит CPE.

4. РАЗВЕРТЫВАНИЕ СЕРВИСА B4N SD-WAN

SD-WAN контроллер и SD-WAN шлюзы могут быть развернуты в системе в виде VNF или PNF. В отличие от VNF, для развертывания и оркестрации PNF не требуется VIM.

Первым шагом при развертывании сервиса SD-WAN является загрузка виртуальной или физической сетевой функции (VNF или PNF) SD-WAN в каталог оркестратора.

4.1. VNF SD-WAN и шаблон сетевого сервиса SD-WAN

VNF SD-WAN состоит из трех функциональных компонентов:

- SD-WAN Controller;
- SD-WAN Gateway1;
- SD-WAN Gateway2.

Каждый компонент размещается в отдельной виртуальной машине, или VDU (Virtual Deployment Unit).

VNF загружаются в систему в виде пакета VNF (VNF Package). Пакет VNF представляет собой архив (tar или zip), содержащий информацию, необходимую для развертывания и управления жизненным циклом VNF.

Пакет VNF SD-WAN включает в себя:

- образы виртуальных машин SD-WAN Controller и SD-WAN шлюз (в формате qcow2);
- VNF дескриптор (в формате XML (vnfd.xml);
- папку со скриптами (“scripts”), которые необходимы для начального развертывания VNF и управления ее жизненным циклом. Для управления конфигурацией VDU используются сценарии Ansible playbook.

Существуют два варианта пакета VNF SD-WAN - с одним контроллером и с кластером контроллеров, состоящим из трех узлов.

После того, как VNF SD-WAN появилась в каталоге, ее можно использовать для создания шаблона сервиса SD-WAN. Для этого нужно с помощью мыши перетащить необходимые элементы сервиса (VNF, виртуальные линки и абстрактные точки подключения) из каталога в окно графического конструктора сервисов и соединить их между собой в соответствии с требуемой топологией. Имеется возможность просмотреть и отредактировать основные параметры VNF и VDU, например, IP адреса и порты для подключения CPE. Далее шаблон сохраняется под уникальным именем и может использоваться для развертывания сервиса SD-WAN (Рис. 7).

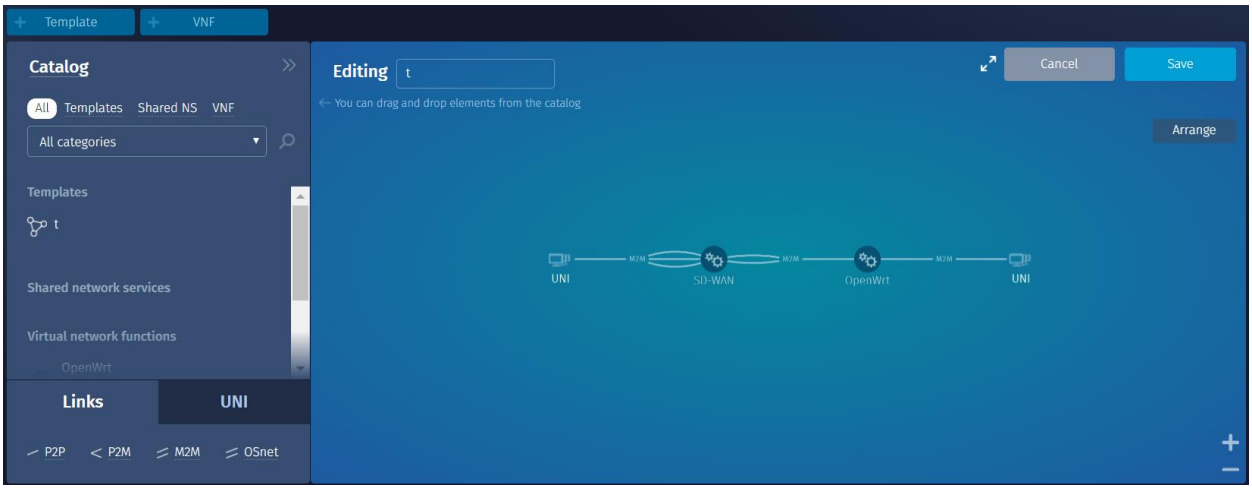

Рис. 7. Шаблон сетевого сервиса SD-WAN

4.2. PNF SD-WAN

В случае, если SD-WAN используется в виде PNF, пакет PNF также представляет собой архив, как и VNF Package, но, в отличие от VNF, в архиве отсутствует папка images, а файл дескриптора называется pnfd.xml. В остальном состав аналогичен VNF Package.

Перед добавлением PNF SD-WAN в каталог необходимо вручную развернуть SD-WAN контроллер (или кластер контроллеров) и два SD-WAN шлюза.

Для PNF оркестратор не создает виртуальные линки, поэтому сетевые интерфейсы и IP связность с оркестратором и между компонентами PNF должны быть настроены администратором заранее.

Если планируется использовать PNF в сервисных цепочках, необходимо до развертывания сервиса добавить соответствующие точки подключения (Connection Points). В этом случае в качестве Connection Point указываются сервисные интерфейсы (коммутатор, порт, VLAN ID). Задавать IP адреса не требуется.

На одну точку подключения Connection Point можно указать несколько сервисных интерфейсов.

Допустимо не указывать сервисные интерфейсы. В этом случае нельзя будет создавать сервисные цепочки с этой PNF в графическом конфигураторе. Пример работающего сервиса SD-WAN без указанных для PNF точек подключения приведен на рис. 8.

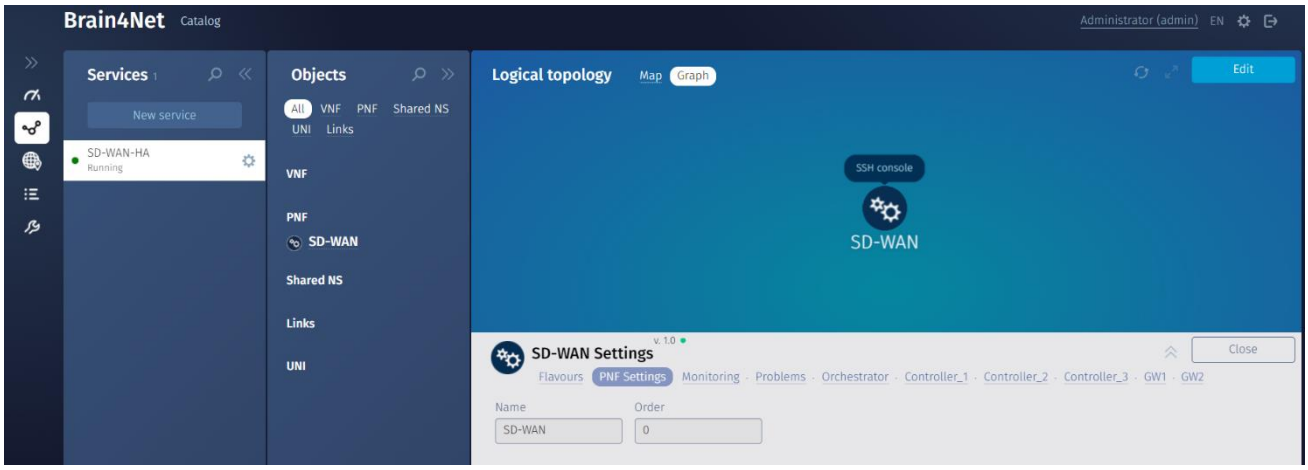

Рис. 8. Сервис SD-WAN с PNF без точек подключения

4.3. Шаблон инстанса SD-WAN (SD-WAN Instance template)

Шаблон инстанса SD-WAN (SD-WAN Instance template) содержит настройки для наложенной (overlay) SDN сети и применяется к контроллеру SD-WAN после развертывания сервиса SD-WAN.

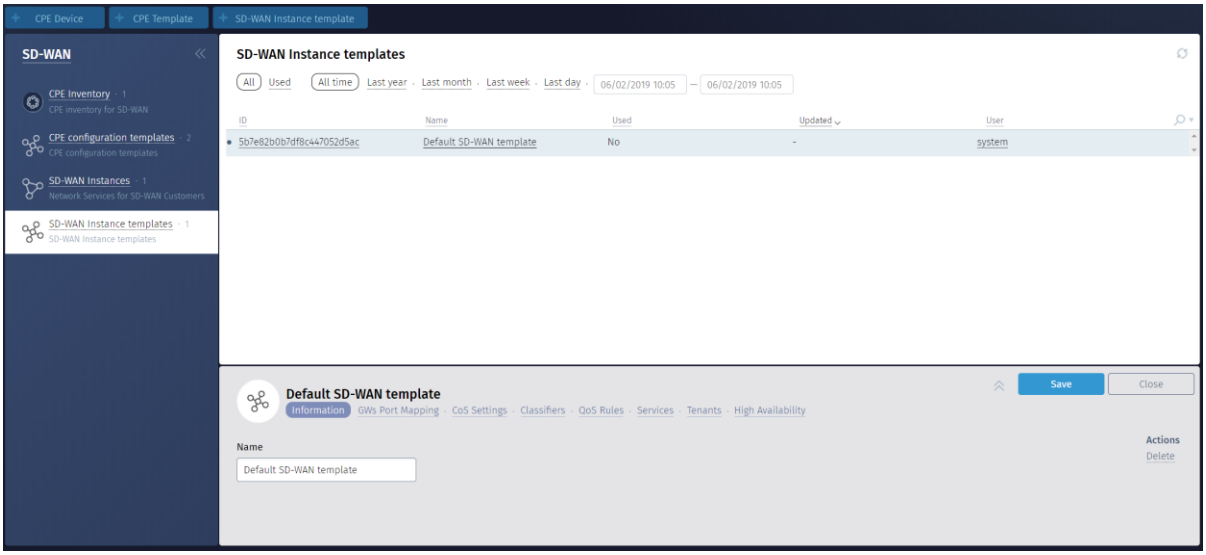

Рис. 9. SD-WAN Instance template

Шаблон состоит из следующих разделов (Рис. 9):

- GWs Port Mapping - список портов SD-WAN шлюзов, которые будут использованы для создания транспортных сервисов в сети SDN;
- CoS Settings, Classifiers, QoS Rules - описание требований к качеству обслуживания;
- Services - информация, необходимая для автоматического создания транспортных сервисов;
- Tenants - список тенантов, к которым привязан шаблон;
- High Availability - выбор количества узлов SD-WAN контроллера.

В разделе GWs Port Mapping перечисляются номера OpenFlow портов шлюзов SD-WAN GW1 и SD-WAN GW2, которые будут использоваться для создания транспортных сервисов.

Настройки QoS включают в себя следующие разделы:

- CoS Settings - позволяет задать классы обслуживания, которые будут использоваться в сети SDN. Всего может быть создано до 8 классов обслуживания, но только один класс должен быть выделен для трафика реального времени. Для каждого класса задается внутренняя (служебная) метка (Internal Tag) и назначается очередь для обработки трафика данного класса.

  Коэффициент переподписки (KOver) рекомендуется оставлять равным “1” для всех классов трафика, кроме Best Effort. Рекомендованное значение максимальной резервируемой полосы пропускания (Max Reserved Bandwidth) - 90%.

- Classifiers - раздел позволяет создать один или несколько классификаторов трафика. Классификатор определяет, доверять или нет меткам качества обслуживания, которые выставлены во входящих пакетах. Если система доверяет значению QoS, то необходимо указать соответствие значений полей DSCP или VLAN PCP ранее определенным классам обслуживания.

- QoS Rules - позволяет ограничить полосу пропускания для входящего в транспортный сервис трафика, в том числе указать доступную полосу пропускания для каждого класса трафика в процентах от общей полосы. Можно создать одно или несколько правил.

В разделе Services создаются шаблоны транспортных SDN-сервисов, которые будут использоваться для передачи данных между CPE и SD-WAN шлюзами. Доступны следующие типы сервисов: L2 P2M (Point-to-Multipoint), L2 M2M (Multipoint-to-Multipoint), L3VPN.

Сервисы P2M и M2M могут содержать две или более точек подключения (сервисные интерфейсы). Отличие сервиса P2M в том, что каждой точке подключения присваивается роль: Root или Leaf. Роль накладывает ограничения на прохождение трафика:

- Пакет, пришедший на порт Root, может быть направлен в порт с любой ролью;
- Пакет, пришедший на порт Leaf, может быть направлен только в порт Root.

Для сервиса выбирается правило QoS Rule из ранее созданных правил.

Точки подключения к сервису определяются указанием устройства, порта, типа инкапсуляции (Access, VLAN, QinQ), значением VLAN ID для инкапсуляции VLAN, значением внешнего и внутреннего VLAN ID для инкапсуляции QinQ.

В данном шаблоне указываются только сервисные интерфейсы на SD-WAN шлюзах. При подключении CPE принадлежащие им сервисные интерфейсы будут автоматически добавлены к сервисам. Список сервисов и параметры сервисных интерфейсов указываются в шаблоне CPE.

Шаблон SD-WAN Instance template должен обязательно содержать один сервис P2M для управления сетью SD-WAN (Management-P2M).

В разделе Tenants можно добавить или удалить тенанты, которые будут использовать данный шаблон. Если для тенанта не планируется использовать шаблон по умолчанию, то требуемый шаблон привязывается к тенанту до развертывания сервиса SD-WAN.

В системе может быть создано несколько шаблонов SD-WAN Instance template, но один из них обязательно должен являться шаблоном по умолчанию.

При развертывании платформы B4N Service Platform автоматически создается шаблон SD-WAN Instance template по умолчанию. Его нельзя удалить, но можно назначить другой шаблон в качестве шаблона по умолчанию.

Если при развертывании сервиса SD-WAN для тенанта к этому тенанту явно не привязан ни один шаблон, то к сервису применяется шаблон по умолчанию.

Шаблон SD-WAN Instance template по умолчанию содержит следующие настройки:

- GWs Port Mapping:
    - GW1 Port = 1 (подключается к сети управления)
    - GW1 Port = 3 (подключается к локальной сети ЦОД)
    - GW2 Port = 1 (подключается к сети управления)
    - GW2 Port = 3 (подключается к локальной сети ЦОД)
- QoS - весь трафик попадает в класс Best Effort, полоса пропускания не ограничивается (Unlimited-QoS);
- Services - автоматически создаются два сервиса с параметрами, приведенными в таблице *1*.

Таблица 1. Сервисы по умолчанию

Параметр	**Сервис 1**	**Сервис 2**
Имя	SD-WAN managementTunnel	SD-WAN P2M Data
Тип сервиса	P2M	P2M
Session / Tunnel / MAC idle timeout (s)	900 / 900 / 3600	900 / 900 / 3600
MAC table size	2000	2000
MAC learning	Classic	Classic
Сервисные интерфейсы (Endpoints SI)	GW1, Port 1, Access, QoS Unlimited-QoS, Role ROOT, Reserve: GW2, Port 1, Access	GW1, Port 3, Access, QoS Unlimited-QoS, Role ROOT, Reserve: GW2, Port 3, Access

4.4. Шаблон CPE

4.4.1. Типы CPE

CPE могут быть двух типов:

1. Стандартные
2. uCPE - с возможностью запуска VNF непосредственно на устройстве.

При добавлении шаблона CPE необходимо указать, для какого типа CPE он создается.

4.4.2. Назначение и разделы шаблона CPE

Шаблон CPE описывает основные параметры CPE и действия, которые необходимо выполнить при начальной конфигурации устройства, его удалении или в других ситуациях.

Шаблон состоит из следующих разделов (Рис. 10):

- Information - имя шаблона;
- Port Mapping - соответствие номеров OpenFlow портов их назначению;
- Activation - состояние устройства по умолчанию (enabled / disabled);
- Deactivation – действия при пропадании связи с CPE (блокирование или удаление);
- Configurations - учетные данные и скрипты для настройки и изменения конфигурации устройства;
- Monitoring - способ мониторинга (Zabbix агент или SNMP) и шаблон мониторинга в сервере Zabbix;
- Services - информация для автоматического включения CPE в SDN-сервисы;
- Consoles - включение доступа к SSH и Web консоли CPE;
- VIM - параметры, используемые для подключения VIM на uCPE. Раздел отображается только в шаблонах для uCPE.

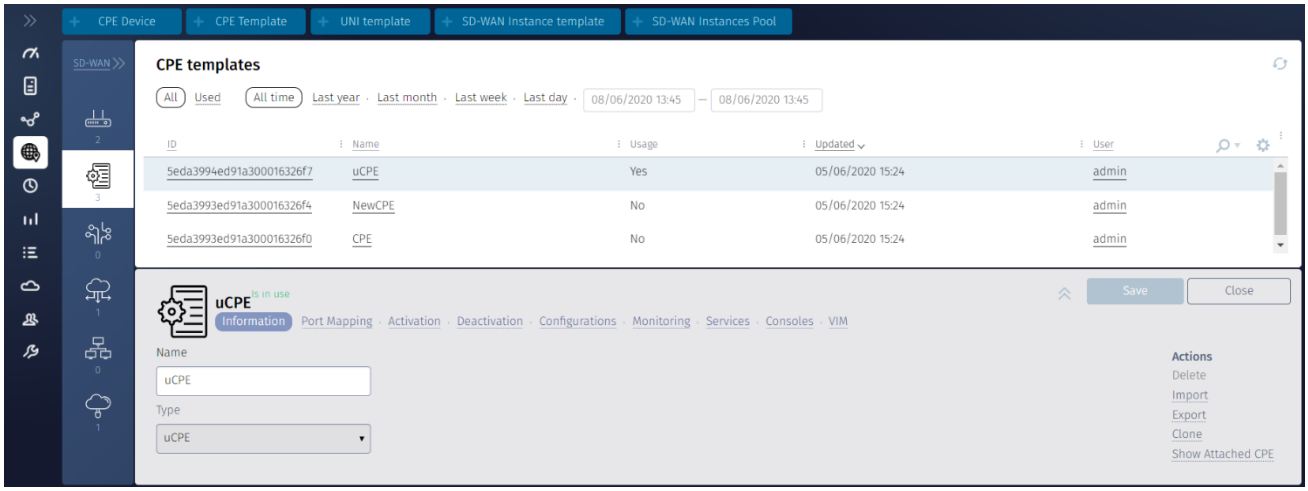

Рис. 10. CPE template

При создании нового шаблона CPE для него автоматически генерируется имя в формате “Template №”, которое может быть изменено администратором. По умолчанию в раздел Port Mapping добавляются порты:

- Management OF port number - 1
- Lan OF port number - 2
- Openstack Data - 3 (только для шаблона uCPE)

В разделе “Activation” задается состояние устройства по умолчанию. Если указано “Enabled”, при подключении CPE автоматически инициируется процедура регистрации, и CPE переходит в активное состояние. Если состояние по умолчанию “Disabled”, CPE регистрируется, но автоматически не активируется. Администратор может вручную активировать CPE, например, после предварительной проверки, что именно эта CPE установлена на площадке клиента.

В разделе “Deactivation” указываются параметры для функции отключения и удаления CPE по таймауту отсутствия связи с SD-WAN контроллером. Эта функция может быть включена в следующих целях:

- Защита от кражи CPE
- Очистка инвентаризационной базы данных от устаревших записей CPE

Раздел “Configurations” позволяет указать, какие скрипты необходимо выполнить при инициализации CPE. Если для выполнения скриптов требуются дополнительные файлы, их также можно импортировать в виде архива .tar.gz или .zip.) Внутри архива должна быть одна корневая папка, которая может содержать другие папки или файлы.

После того как CPE регистрируется в оркестраторе, VNF Manager ожидает, когда CPE станет доступной через сеть управления (SD-WAN managementTunnel), и выполняет скрипты.

Для начального доступа на CPE задаются логин и пароль по умолчанию, а также порт SSH. Впоследствии эти параметры заменяются на автоматически сгенерированные значения.

При добавлении конфигурации имеется возможность выбрать executor (Ansible, Expect, Custom), состояние CPE, в котором необходимо применить конфигурацию (инициализация, удаление устройства), и импортировать файл со скриптом или сценарием Ansible playbook.

Шаблон uCPE имеет дополнительную вкладку VIM (Рис. 11). Программное обеспечение, предустановленное на uCPE, содержит менеджер виртуальной инфраструктуры OpenStack, который будет использоваться для запуска виртуальных машин. На вкладке VIM указываются параметры, используемые оркестратором при взаимодействии с VIM на uCPE.

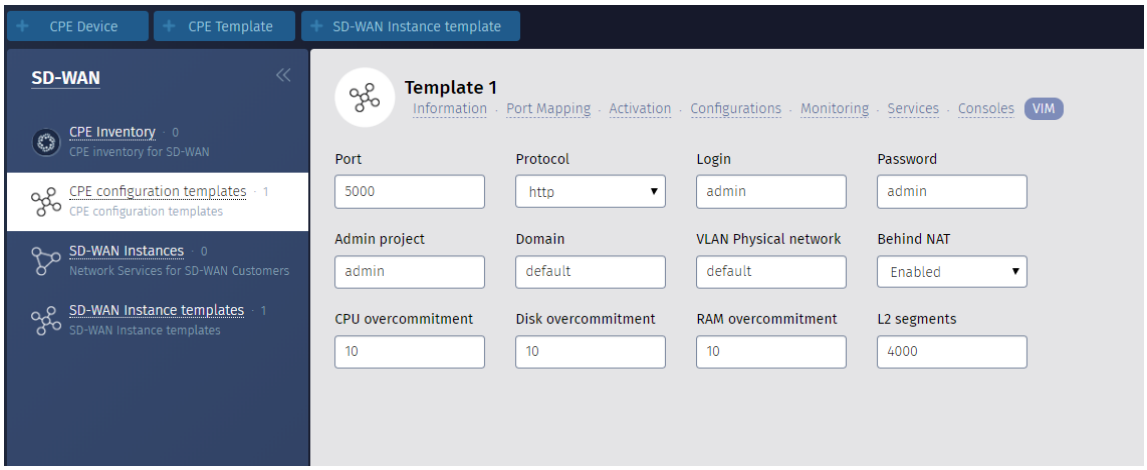

Рис. 11. Вкладка VIM шаблона CPE

Шаблон привязывается к CPE на этапе активации устройства. Шаблон не может быть удален, если есть CPE, которые его используют. Шаблон может быть отвязан от CPE только путем удаления CPE.

4.4.3.Операции с шаблонами CPE

С шаблонами CPE могут производиться следующие действия:

1. Создание
2. Изменение
3. Удаление
4. Экспорт/Импорт
5. Клонирование
6. Просмотр списка CPE, использующих данный шаблон.

4.4.3.1.Экспорт и импорт шаблонов CPE

Экспорт осуществляется в архив в формате tar.gz. В архиве содержатся:

- файл в формате xml, описывающий шаблон CPE
- файлы скриптов
- файлы для использования при выполнении скриптов (например, SSL сертификаты)

Экспортированный шаблон содержит все разделы шаблона CPE:

- Information
- Port Mapping
- Activation
- Deactivation
- Configurations
- Monitoring
- Services

Связи шаблона с тенантами не экспортируются.

Импорт шаблона возможен из архива zip или tar.gz. Можно выбрать импорт всех разделов, либо указать один или несколько интересующих. При этом будут заменены параметры только выбранных разделов. Импортируемый раздел заменяется полностью.

Импорт может производиться в конкретный уже созданный шаблон CPE. Если нужен новый шаблон, то сначала нужно его создать и потом осуществить в него импорт.

При импорте в шаблон, к которому привязаны CPE, эти связи сохраняются. С привязанными к шаблону CPE не происходит никаких изменений в момент импорта настроек.

4.4.3.2.Клонирование шаблонов CPE

При клонировании шаблона создается полная копия шаблона, с изменением его имени и ID. Клонируются все разделы шаблона, включая скрипты и файлы. Связи шаблона с CPE и тенантами не переносятся в клонированный шаблон.

4.5. Создание тенанта

Тенант представляет собой логический набор ресурсов, предоставляемых Заказчику или выделяемых из общего пула с какой-либо другой целью. Каждый тенант содержит набор точек подключения (пользовательские сетевые интерфейсы - UNI), виртуальные сетевые функции из каталога, которые могут быть использованы для создания сервисов, ЦОД, где находятся вычислительные ресурсы, и группу VIM, под управлением которых будут работать виртуальные функции VNF.

К каждому тенанту привязываются учетные записи. Администратор тенанта в рамках выделенных ему ресурсов может выполнять следующие функции:

- просмотр топологии и переход к управлению выбранным компонентом сети,
- создание, удаление и редактирование сетевых сервисов в Конфигураторе сервисов, просмотр загрузки компонентов,
- управление виртуальными сетевыми функциями,
- мониторинг системы.

Администратор платформы имеет возможность подключиться к тенанту в качестве администратора тенанта для настройки и устранения неполадок.

При создании тенанта администратор платформы выделяет тенанту необходимые ресурсы:

1. Добавляет один или несколько VIM, при необходимости ограничивает доступные вычислительные ресурсы;
2. Создает для тенанта точки подключения (UNI);
3. Назначает пользователей с правами администратора тенанта;
4. Предоставляет право использования шаблона сервиса SD-WAN из каталога.

В качестве точек подключения указываются сервисные интерфейсы (коммутатор OpenFlow, порт, инкапсуляция), через которые трафик клиента будет попадать из локальной сети ЦОД в сетевой сервис.

4.6. Развертывание сервиса SD-WAN для тенанта

Чтобы активировать сервис SD-WAN, администратору тенанта необходимо в портале самообслуживания выбрать в каталоге шаблон сервиса SD-WAN и перетащить его в окно графического конструктора сервисов для редактирования. Абстрактные точки подключения UNI должны быть заменены на реальные, которые предварительно были созданы и привязаны к тенанту администратором платформы. Далее необходимо присвоить сервису имя и сохранить его.

После этого администратор тенанта может развернуть сервис (Рис. 12) и приступить к подключению CPE.

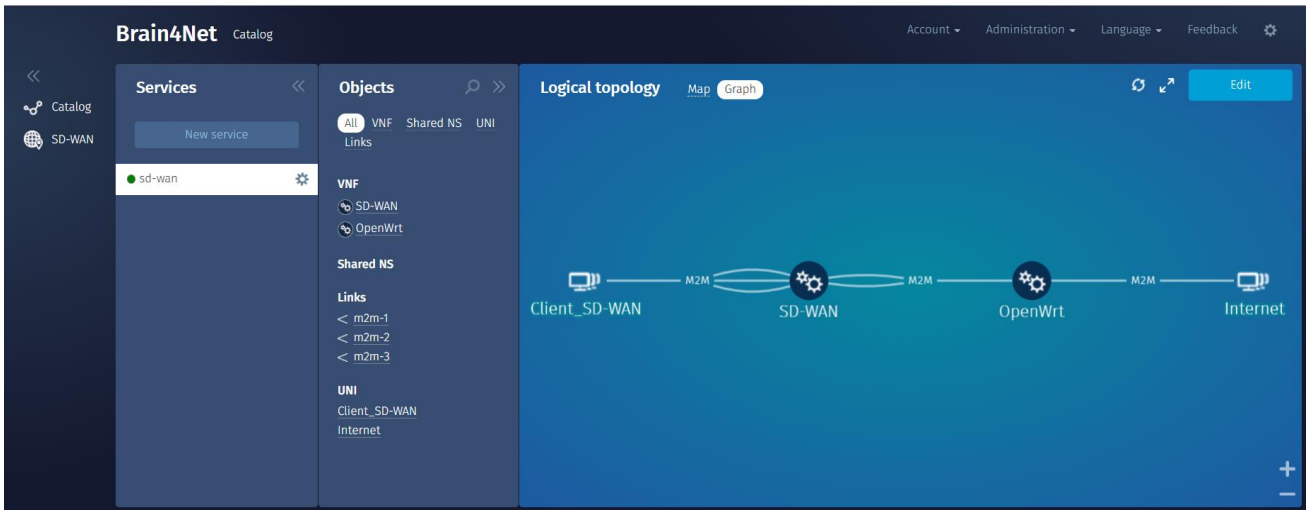

Рис. 12. *Развертывание сервиса SD-WAN*

4.7. Регистрация CPE

Схема регистрации CPE приведена на Рис. 13.

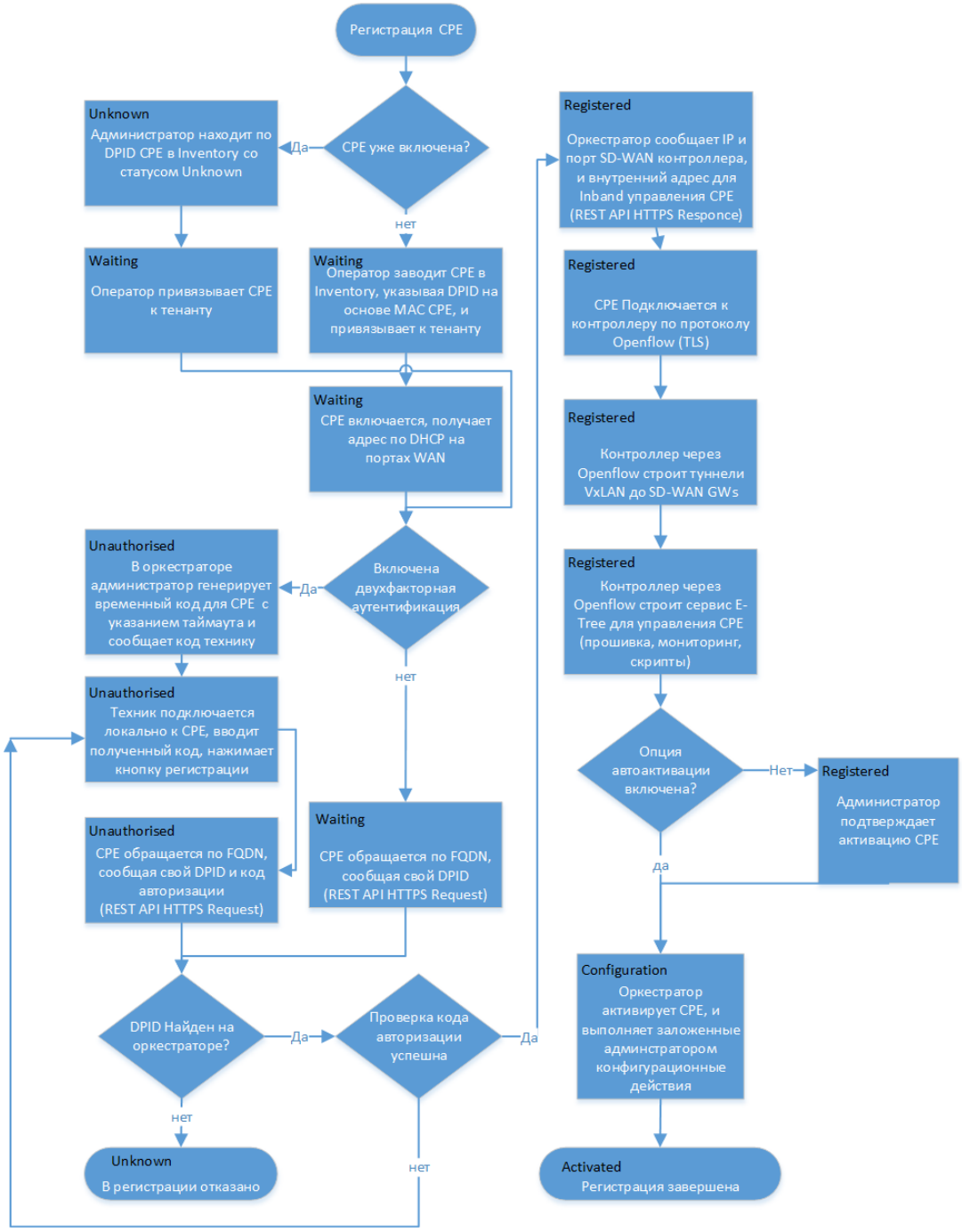

Рис. 13. Процесс регистрации CPE

5. ИНВЕНТАРИЗАЦИОННАЯ БАЗА CPE

5.1. Добавление CPE в инвентаризационную базу

Объект “CPE device” в инвентаризационной базе оркестратора (CPE Inventory) представляет собой аппаратное устройство CPE на сайте заказчика, на котором предустановлено соответствующее программное обеспечение.

CPE добавляется в CPE Inventory перед отправкой заказчику. Уникальный идентификатор CPE резервируется за заказчиком (привязывается к тенанту).

При добавлении CPE в инвентаризационную базу администратор указывает следующие параметры:

- Уникальный идентификатор (DPID);
- Имя;
- Расположение (адрес площадки);
- Шаблон конфигурации CPE;
- Тенант.

При формировании DPID могут использоваться различные идентификаторы устройства, например, MAC адрес первого WAN интерфейса или серийный номер.

После ввода необходимой информации новое устройство CPE появляется в таблице CPE Inventory со статусом "waiting" (Рис. 14). Остальные характеристики CPE (IP адрес и порт SD-WAN контроллера и шлюзов) заполняются автоматически. В дальнейшем CPE можно редактировать, блокировать или удалить.

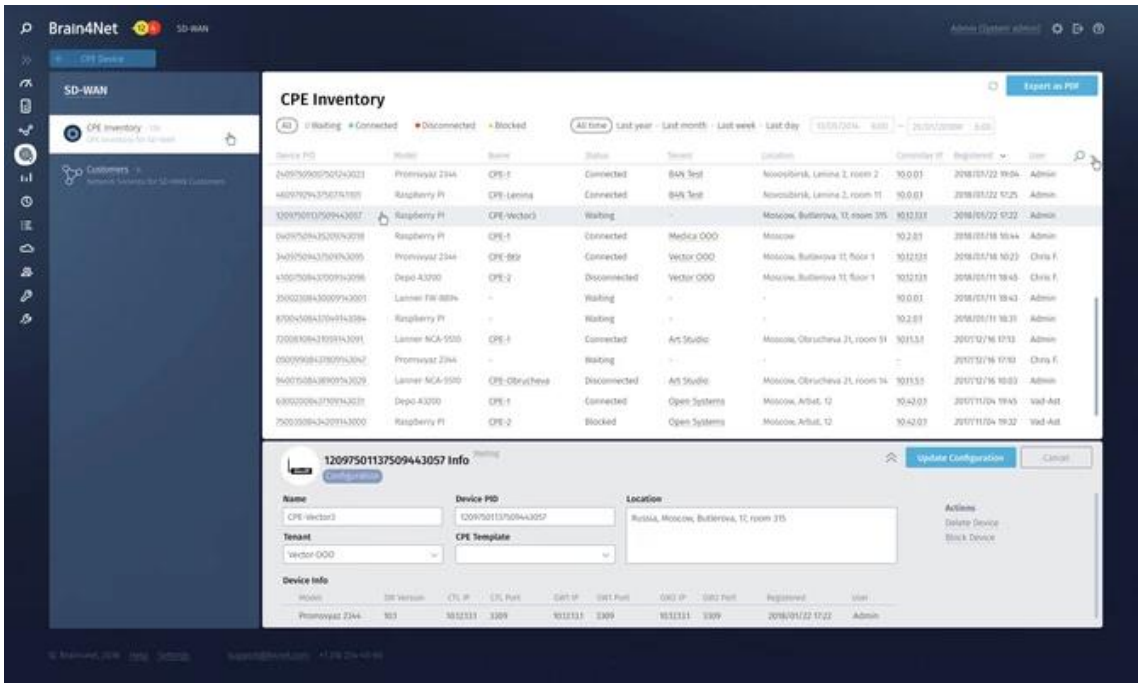

Рис. 14. *Инвентаризационная база CPE*

После установления соединения CPE с оркестратором и получения необходимой конфигурационной информации статус устройства в CPE Inventory меняется на “Registering”. Успешно подключившиеся к SD-WAN контроллеру CPE имеют статус “Registered”.

Объект “CPE device” имеет следующие параметры:

- DPID - уникальный идентификатор CPE, вводится предварительно администратором. При регистрации CPE передает свой DPID по API оркестратору для сопоставления.
- Model - модель устройства, передается от CPE оркестратору по API.
- SW Version - версия программного обеспечения CPE, передается от CPE оркестратору по API.
- CPE Template – шаблон, использованный при регистрации CPE.
- Name - имя CPE, может быть не уникальным. Генерируется автоматически на основании порядкового номера в рамках тенанта по шаблону CPE-X, где X принимает значения 1,2,3 и т.д. Может быть изменено администратором.
- Status - текущий статус устройства:
    - Unknown - CPE пытается подключиться к оркестратору, но ее DPID отсутствует в CPE Inventory
    - Waiting - Запись для CPE заведена в CPE Inventory, но CPE пока не подключена
    - Registering - CPE находится в процессе регистрации
    - Error - процесс регистрации завершился ошибкой
    - Registered - CPE успешно зарегистрирована
    - Configuration - на CPE меняется конфигурация
- State - Enabled или Disabled. Состояние по умолчанию задается шаблоне CPE и может быть изменено до регистрации CPE.
- Connection – Connected или Disconnected. Есть ли связь с устройством в данный момент.
- Usage - параметр, показывающий, используется ли CPE в каких-либо сервисах. Может иметь значение Yes, No. Блокирующий параметр, не позволяющий удалить CPE, использованную в сервисе.
- Transport Tenant – транспортный тенант, которому принадлежит устройство.
- Customer Tenant – клиентский тенант к которому привязана CPE.
- Location - адрес размещения CPE (привязка к карте).
- Management IP – IP адрес устройства в сети управления.
- Controllers - публичный IP адрес и порт SD-WAN контроллера, используется для подключения CPE, SD-WAN шлюзов, взаимодействия с оркестратором.
- Gateways - публичные IP адреса и порты SD-WAN шлюзов, используются для построения VXLAN туннелей от CPE и взаимодействия с SD-WAN контроллером.

- Mobile Network – мобильные операторы для каждой установленной в CPE SIM-карты.
- Registered - дата и время регистрации CPE в CPE Inventory.
- Update – дата и время последнего изменения статуса CPE.
- User – имя пользователя, зарегистрировавшего CPE.

Если в оркестратор пришел запрос от неизвестной CPE (DPID не совпадает ни с одной записью), то она добавляется в список CPE Inventory со статусом Unknown.

Для выполнения задач, связанных с эксплуатацией и обслуживанием устройств CPE, имеется возможность гибкой группировки и поиска устройств с заданными характеристиками.

В таблице CPE Inventory администратор может выбрать столбцы для отображения, сортировать и выполнять поиск по любому параметру.

Каждому устройству назначаются метки, например, модель, версия ПО, тип офиса или площадки, географическое расположение. Часть меток присваивается автоматически, администратор может добавлять новые метки для классификации устройств по своему усмотрению. Метки можно добавлять и удалять как отдельным устройствам, так и группе CPE. Далее администратор, используя одну или несколько меток, может выбрать нужное подмножество устройств, чтобы выполнить с ними необходимые действия (изменить конфигурацию, обновить ПО и т.п.)

При выборе CPE в таблице открывается панель для ее редактирования (Рис. 15).

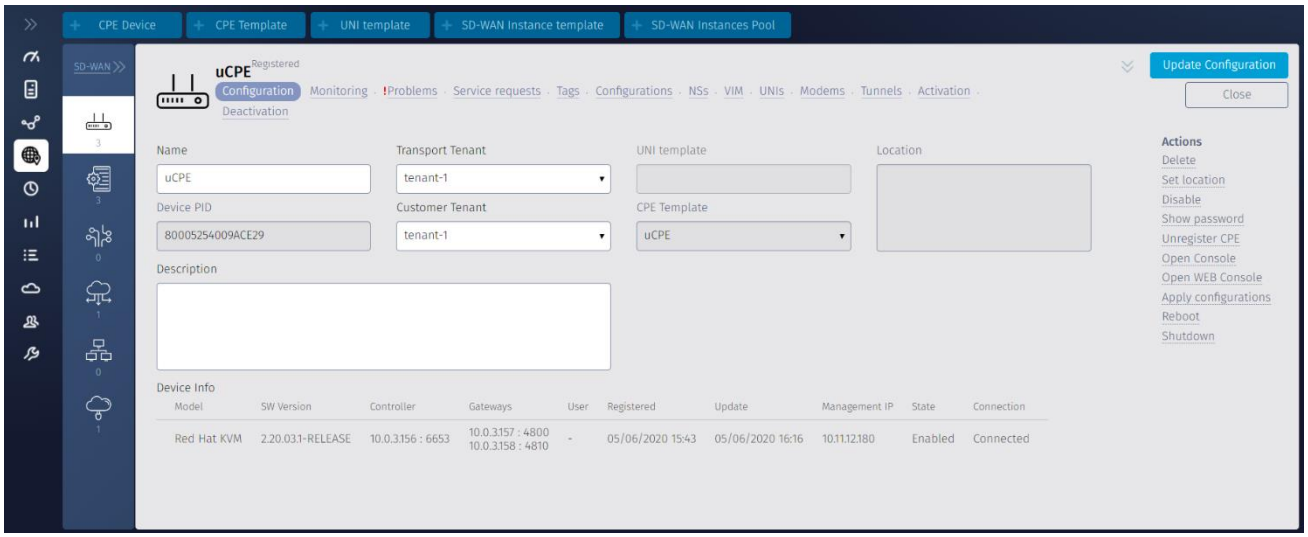

Рис. 15. Редактирование CPE

5.2. Действия с CPE

После того, как CPE добавлена в инвентаризационную базу, администратор может выполнять с ней следующие действия:

- редактировать

- блокировать
- удалить

Действия, доступные при редактировании CPE, зависят от ее статуса. Возможные операции с CPE приведены в табл. *2*.

Таблица 2. Действия с CPE

Статус CPE	**Возможные действия**
Unknown	Delete Register
Waiting	Delete Set Location
Registering	None
Error	Delete
Registered	Delete Set Location Enable/Disable Show password Unregister CPE Open Console Open WEB Console Apply Configuration Reboot Shutdown
Configuration	Set Location Show Password Open Console

Удаление CPE возможно, если параметр Usage имеет значение “No”, то есть CPE не используется в сервисах. При удалении CPE соответствующий ей коммутатор удаляется из базы данных SD-WAN контроллера, очищается принадлежность тенанту, удаляется запись в CPE Inventory. Перед удалением CPE необходимо ее заблокировать (выполнить действие Disable).

6. СОСТАВ И ОПИСАНИЕ SD-WAN GATEWAY И SD-WAN CPE

6.1. Описание SD-WAN шлюзов

Сервис SD-WAN включает в себя два шлюза - основной и резервный. Шлюзы разворачиваются на разных VDU и соединяются каналом Ethernet с прозрачным пропуском заголовков VLAN (802.1q/802.1ad).

Шлюзы SD-WAN подключаются к сети Интернет. Каждому шлюзу может быть назначен выделенный IP адрес, маршрутизируемый в сети Интернет, или для обоих шлюзов может использоваться один IP адрес, но разные порты UDP.

Логическая схема шлюзов приведена на Рис. 16.

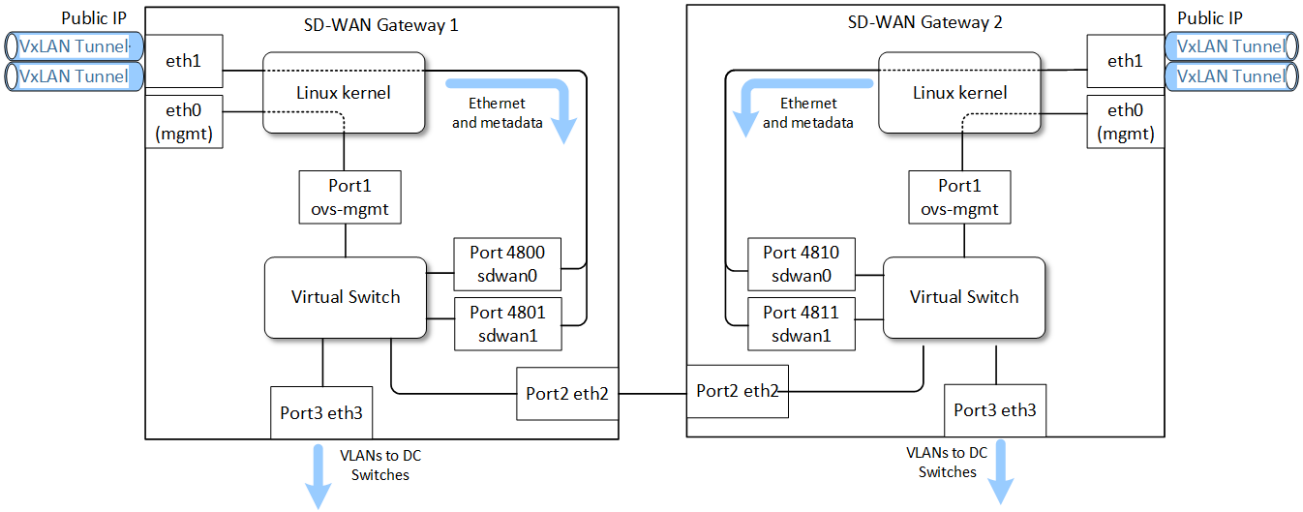

Рис. 16. Логическая схема шлюзов SD-WAN

Каждый шлюз SD-WAN содержит 4 порта Ethernet:

- eth0 - порт для управления шлюзом;
- eth1- порт, используемый для терминации VxLAN туннелей от CPE;
- eth2 - порт для объединения шлюзов, необходим для корректной работы резервирования.
- eth3 - порт для подключения к локальной сети ЦОД. Используется для создания виртуальных линков к другим VNF или для выхода в Интернет.

В состав шлюза входит программный коммутатор OpenFlow. Порты eth2, eth3 включаются напрямую в виртуальный коммутатор. Порты sdwan0 и sdwan1 имеют тип VXLAN со следующими параметрами:

- в качестве source IP назначается IP адрес, настроенный на порту eth1;
- номера портов для первого шлюза равны 4800 и 4801;
- номера портов для второго шлюза - 4810 и 4811.

Если CPE, которые планируется подключать к шлюзам, имеют более двух WAN портов, соответственно увеличивается и количество sdwan интерфейсов на шлюзах. Номера портов присваиваются следующие по порядку.

Программный коммутатор OpenFlow управляется SD-WAN контроллером и содержит следующие OpenFlow-порты :

1. Port 1 (Port mgmt) - включается в сервис P2M SD-WAN Management;
2. Port 2 (eth2) - транзитный порт, не используется для создания сервисов;
3. Port 3 (eth3) - используется для создания сервисов, участвующих в передаче трафика данных от CPE;
4. Порты 4800 - 4801 (4810 - 4811 для SD-WAN GW2) - транзитные порты.

6.2. Описание CPE

Логическая схема CPE приведена на Рис. 17.

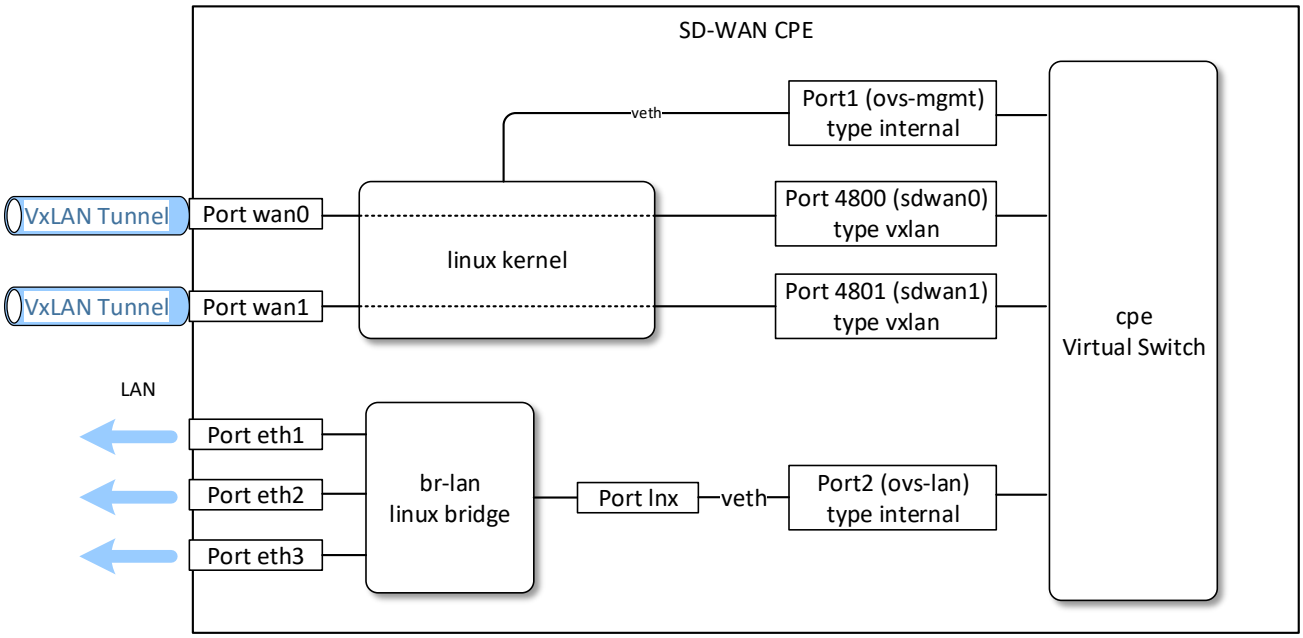

Рис. 17. Логическая схема CPE

Внешние порты CPE включают в себя:

- один или более портов LAN, которые могут быть объединены в коммутатор на основе linux bridge;
- один или более портов WAN, которые могут иметь разную среду передачи (проводную или беспроводную). На каждом из портов ожидается получение настроек IPv4 по протоколу DHCP.

Для удаленной настройки CPE после ее подключения к оркестратору и контроллеру SD-WAN организуется внутренний порт mgmt.

На CPE устанавливается программный коммутатор OpenFlow (CPE Virtual Switch), управляемый SD-WAN контроллером. Коммутатор имеет следующие OpenFlow-порты:

- Port 1 (ovs-mgmt) - для организации inband управления и настройки CPE после подключения CPE к контроллеру SD-WAN через специальный служебный сервис (SD-WAN managementTunnel);
- Port 2 (ovs-lan) - порт подключения к linux bridge;
- Порты 4800 и 4801 (sdwan0 и sdwan1) - для каждого порта WAN создается порт типа VXLAN со следующими параметрами: port_no равен 4800 и далее увеличивается на 1 для каждого последующего

WAN-порта, source IP - назначается IP адрес соответствующего WAN-интерфейса, destination port - назначается равным port_no.

После получения на портах WAN настроек по протоколу DHCP на CPE создаются отдельные маршрутные таблицы для каждого из портов.

Количество и тип внешних и внутренних портов CPE, их нумерация, действия по настройке устройства CPE при его инициализации описываются в шаблоне CPE.

6.3. Описание uCPE

Программное обеспечение uCPE устанавливается на стандартный сервер x86 архитектуры и, в дополнение к функциональности SD-WAN, позволяет развертывать виртуальные сетевые функции таким же способом, что и в виртуальной инфраструктуре ЦОД.

uCPE содержит гипервизор и VIM (Openstack в минимальной конфигурации). Остальные необходимые для оркестрации VNF компоненты находятся в ЦОД - оркестратор, SDN контроллер, VNF Manager, система мониторинга.

Взаимодействие оркестратора с VIM на uCPE становится возможным после регистрации CPE и подключения ее к SDN-сервисам, в частности, к сервису SD-WAN managementTunnel. Через этот же сервис осуществляется мониторинг и конфигурация VNF.

Имеется возможность создания сетевого сервиса на uCPE, и когда она недоступна (находится в состоянии “Disconnected”). Для реализации такого отложенного развертывания сетевого сервиса оркестратор отслеживает доступность uCPE и, как только VIM на uCPE начнет отвечать на запросы API, развертывает сервис.

VIM uCPE по умолчанию привязывается к тенанту, в котором развернут сервис SD-WAN, но можно указать и другой тенант. Это необходимо в случаях, когда один SD-WAN инстанс используется несколькими клиентами.

При создании сервиса необходимо выбрать VIM, где развертывать VNF. Это может быть либо привязанный к тенанту VIM в ЦОД, либо VIM на uCPE.

При удалении uCPE удаляются все сервисные цепочки, развернутые на устройстве.

Логическая схема uCPE приведена на Рис. 18.

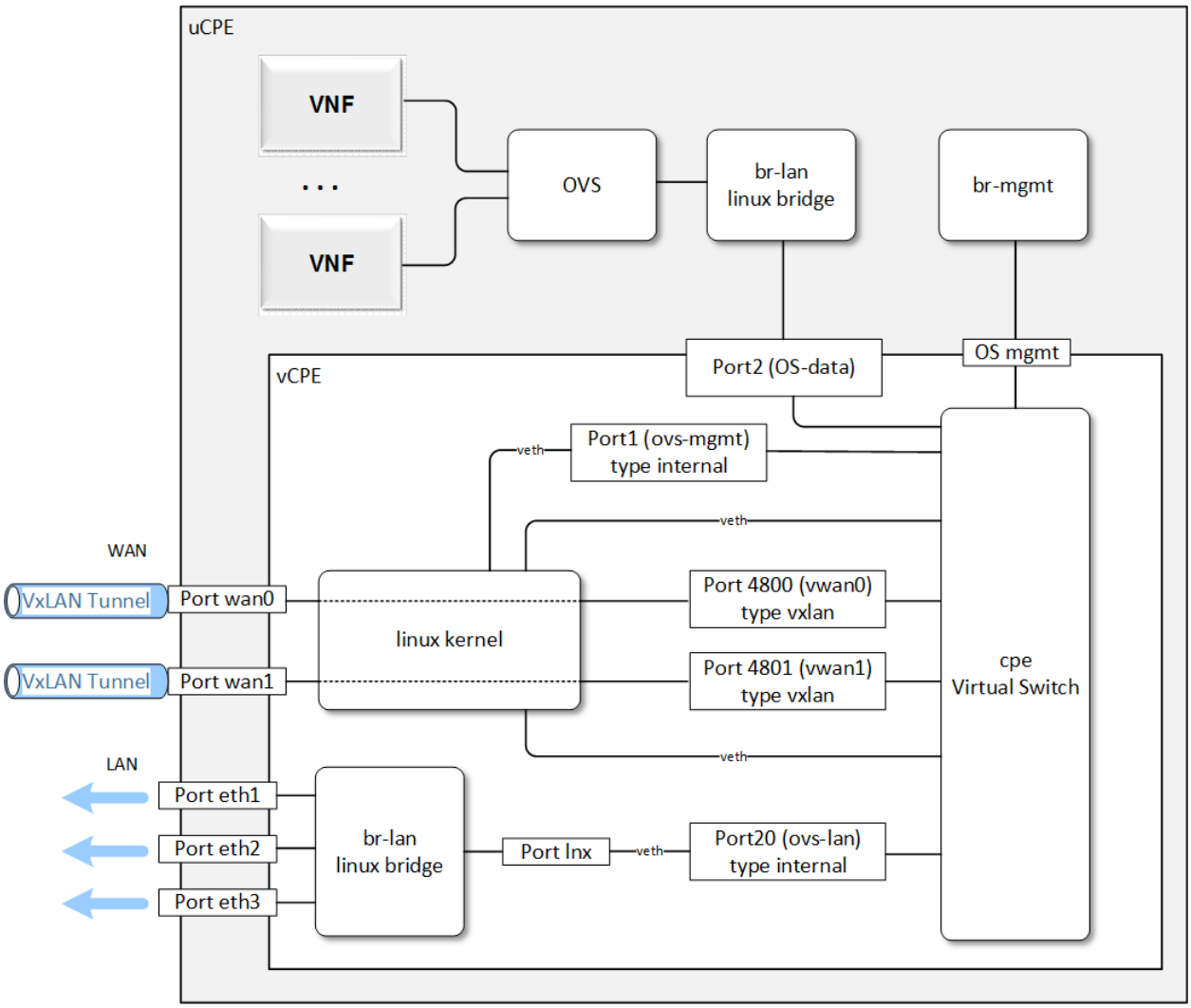

Рис. 18. Логическая схема uCPE

Программный коммутатор OpenFlow, по сравнению с обычным устройством CPE, содержит дополнительный порт OS-data. Для uCPE в шаблоне необходимо указывать следующие номера OpenFlow портов:

- Management OF port number – 1
- Openstack Data – 2
- LAN OF port number - 20

Если используется несколько LAN портов, для них указываются номера 21, 22 и т.д

7. УПРАВЛЕНИЕ И МОНИТОРИНГ CPE

7.1. Управление CPE

Для управления и мониторинга CPE используется выделенная сеть управления. Оркестратор создает на SD-WAN контроллере служебный сервис P2M SD-WAN managementTunnel. Портом root является сервисный интерфейс на SD-WAN шлюзе 1 - port 1 с инкапсуляцией Access. В качестве резервного сервисного интерфейса используется port 1 с инкапсуляцией Access на шлюзе 2.

После того, как CPE подключится к SD-WAN контроллеру, оркестратор создает сервисный интерфейс на порту mgmt CPE с типом Access. Номер порта определяется в шаблоне CPE (по умолчанию порт 1). Оркестратор активирует CPE и добавляет сервисный интерфейс в сервис P2M SD-WAN managementTunnel с ролью leaf (Рис. 19).

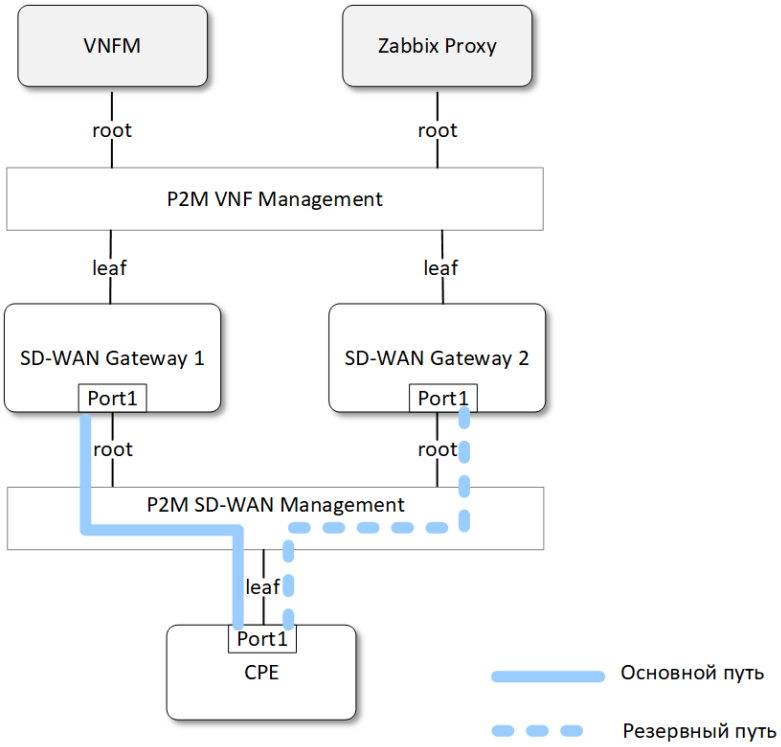

Рис. 19. Сеть управления CPE

IP адрес для управления CPE выделяется автоматически из пула адресов, заданных администратором, и отображается в CPE Inventory. При удалении CPE IP адрес возвращается в пул.

Взаимодействие между компонентами SD-WAN VNF (или PNF) и оркестратором осуществляется через внешние WAN IP адреса.

Из интерфейса оркестратора может быть предоставлен доступ к SSH и/или Web консоли CPE, если данная опция была определена в шаблоне CPE. При этом не требуется иметь связность с CPE по протоколу IP, доступ к консоли проксируется VNFM через сеть управления SD-WAN managementTunnel.

7.2. Мониторинг CPE

Для мониторинга CPE используется внешняя система мониторинга Zabbix, которая включает в себя сервер Zabbix и серверы Zabbix Proxy, устанавливаемые в каждом ЦОД. За мониторинг конкретной CPE отвечает сервер Zabbix Proxy, привязанный к ЦОД (DC), где развернут сервис SD-WAN, к которому подключена данная CPE. Для сбора статистики Zabbix Proxy использует сеть управления P2M SD-WAN managementTunnel.

Мониторинг осуществляется с помощью агента Zabbix или по протоколу SNMP. Способ мониторинга выбирается в шаблоне CPE в разделе Monitoring. Там же указывается шаблон Zabbix (Zabbix Template), который необходимо использовать. Данный шаблон должен быть предварительно создан на сервере Zabbix.

Когда процесс регистрации CPE завершается (CPE подключилась к SD-WAN контроллеру), на сервере Zabbix создается соответствующий хост для мониторинга. При удалении CPE из CPE Inventory, удаляется и хост из Zabbix.

Для просмотра данных мониторинга используется закладка “Monitoring” в окне с информацией о выбранной CPE в CPE inventory (Рис. 20).

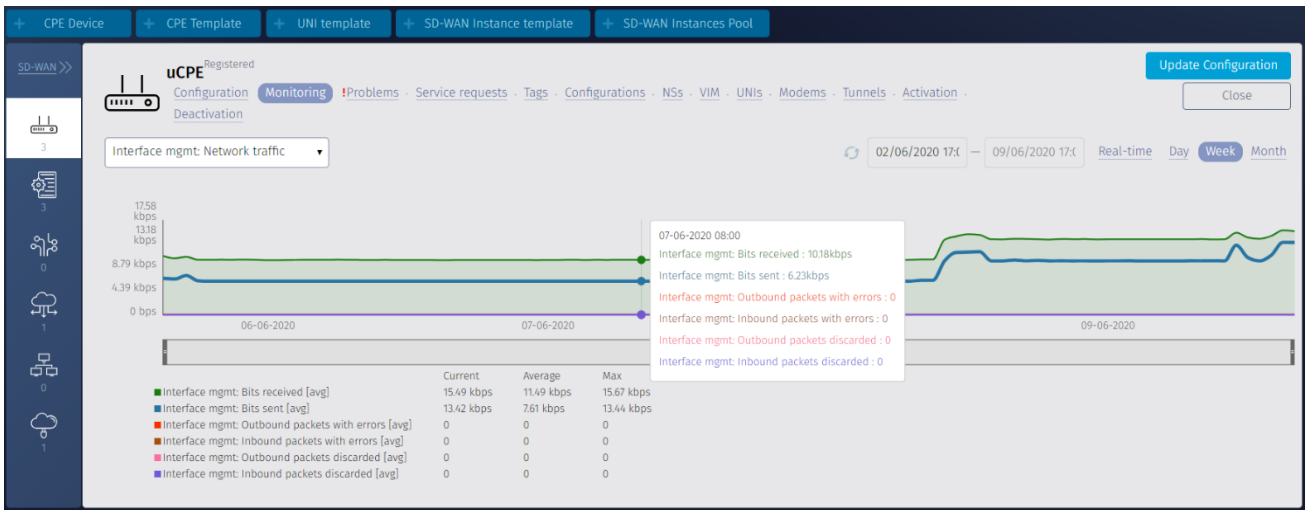

Рис. 20. Мониторинг CPE

Администратор или оператор тенанта могут просматривать графики изменения параметров, для которых включен мониторинг, а также изменять настройки отображения:

- Выбрать график из списка доступных,
- Выбрать интервал (предустановленные интервалы – Real-Time (1 час, обновление раз в секунду), 1 день, 1 неделя, 1 месяц).

7.3. Локальная диагностика CPE

Программное обеспечение CPE содержит встроенный агент (B4N CPE Agent), который собирает информацию о состоянии CPE. Если связь с CPE теряется, локальный пользователь может открыть страницу диагностики CPE и локализовать проблему.

Для получения доступа к странице диагностики необходимо подключиться к LAN интерфейсу CPE и ввести в браузере стандартный служебный IP адрес. По умолчанию это адрес 169.254.254.254/16.

На экран будет выведена Web-страница с результатом диагностики. Предполагается, что локальный пользователь сможет назвать красные блоки, либо их расположение (строка + столбец), либо сделать фотографию и отправить в техническую поддержку.

Страница диагностики CPE, работающей в штатном режиме, приведена на Рис. 21.

Diagnostic page for CPE 8000B827EBBB4860

Connection to GW1	Connection to GW2	Connection to CTL	Switch State
WAN 1 State	WAN 1 Internet Access	WAN 2 State	WAN 2 Internet Access
WI-FI	LAN 1 State	LAN 2 State	LAN 3 State
LAN 4 State	LAN 5 State	LAN 6 State	LAN 7 State

Рис. 21. Страница диагностики CPE, работающей в штатном режиме

Проблемные блоки подсвечиваются красным (Рис. 22).

Diagnostic page for CPE 8000B827EBBB4860

Connection to GW1	Connection to GW2	Connection to CTL	Switch State
WAN 1 State	WAN 1 Internet Access	WAN 2 State	WAN 2 Internet Access
WI-FI	LAN 1 State	LAN 2 State	LAN 3 State
LAN 4 State	LAN 5 State	LAN 6 State	LAN 7 State

Рис. 22. Страница диагностики CPE при наличии проблем

8. УПРАВЛЕНИЕ ТРАФИКОМ

8.1. Использование нескольких путей для передачи трафика

Одним из основных требований к сети SD-WAN является возможность одновременного использования нескольких каналов связи, подключенных к абонентскому устройству. В результате повышается общая скорость подключения и доступность CPE.

SD-WAN контроллер поддерживает технологию использования нескольких путей для передачи трафика (multipathing).

С точки зрения контроллера, связность между двумя узлами сети называется сегментом. Сегмент может содержать один или несколько транспортных путей. Все эти пути начинаются на начальном узле сегмента и оканчиваются на конечном.

Количество путей для одного сегмента может составлять от 2 до 16. Максимальное число путей в сегменте регулируется настройками контроллера. Это значение копируется в параметр Maximum number of paths создаваемых сегментов и может быть переопределено для каждого сегмента.

Путь имеет следующие атрибуты:

- Стоимость (Path.cost) - по умолчанию это сумма стоимости всех линков, входящих в путь, может быть переопределена вручную для путей определенных типов
- Вес (Path.weight)
- Тип (Path.type). Тип пути может принимать следующие значения:
    - Auto-SPF (Shortest-path forwaring) - автоматически рассчитываемый контроллером наилучший маршрут, не может быть создан/изменен/удален пользователем.
    - Manual-TE (Traffic Engineering) - создаваемый вручную путь, администратор указывает все последовательные линки от начального до конечного узла сегмента.
    - Auto-TE - рассчитываемый контроллером основной путь на основании ограничений, заданных пользователем (загрузка линка, уровень ошибок и другие).
- Path.admin.state - административное состояние пути, назначаемое администратором. При значении 'down' путь не используется
- Path.oper.state – фактическое состояние пути в зависимости от возможности передачи трафика. При значении 'down' путь не используется.

Параметры сегмента настраиваются централизовано в шаблоне CPE, при этом есть возможность указать индивидуальные значения на странице настройки отдельной CPE.

Редактируемые параметры сегмента:

- Максимальное количество путей
- Максимальное количество путей Auto-SPF
- Cost variance multiplier - коэффициент, определяющий, во сколько раз большую стоимость по сравнению с наилучшим маршрутом могут иметь пути, чтобы быть включенными в сегмент. Диапазон значений – от 1 до 10.

Чтобы в сегменте учитывались пути с разным весом, необходимо включить параметр “'Enable Multi Weight”. Пример настройки сегмента приведен на Рис. 23

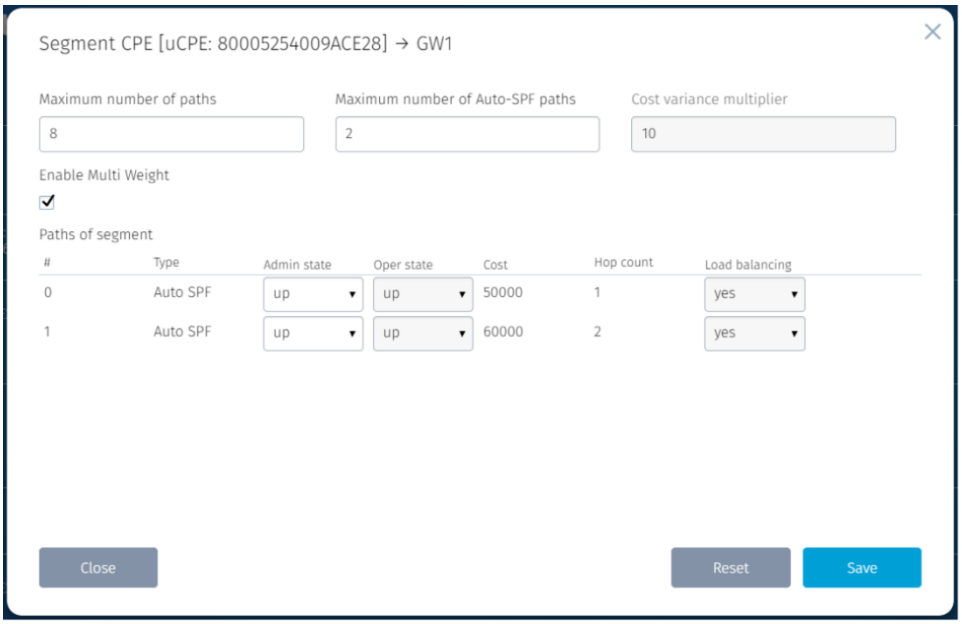

Рис. 23. Редактирование параметров сегментов

Если флажок “'Enable Multi Weight” установлен, трафик будет распределяться по транспортным путям приблизительно пропорционально их весу. При выключенном параметре “'Enable Multi Weight” распределение трафика будет равномерным (Path.weight для всех путей считается равным единице).

8.2. Создание сервисов с SLA

Если для определенных сервисов требуется соблюдение требований SLA, необходимо использовать функцию Constraints.

Constraints являются связующим звеном между определенным сервисом (P2P/P2M/M2M/L3VPN) и пороговыми значениями Thresholds на линках между CPE и SD-WAN шлюзами. Настройка SLA для сервисов выполняется в следующем порядке:

1. Включается мониторинг линков и устанавливаются пороговые значения параметров качества обслуживания
2. Создаются требуемые ограничения (Constraints)
3. В настройках сервиса указываются ранее созданные ограничения.

Чтобы включить мониторинг линков для CPE, необходимо выбрать устройство в CPE Inventory и перейти на вкладку Tunnels. Далее выбрать требуемый линк и нажать «Management» - «Set link level thresholds». Окно настройки мониторинга линков приведено на Рис. 24

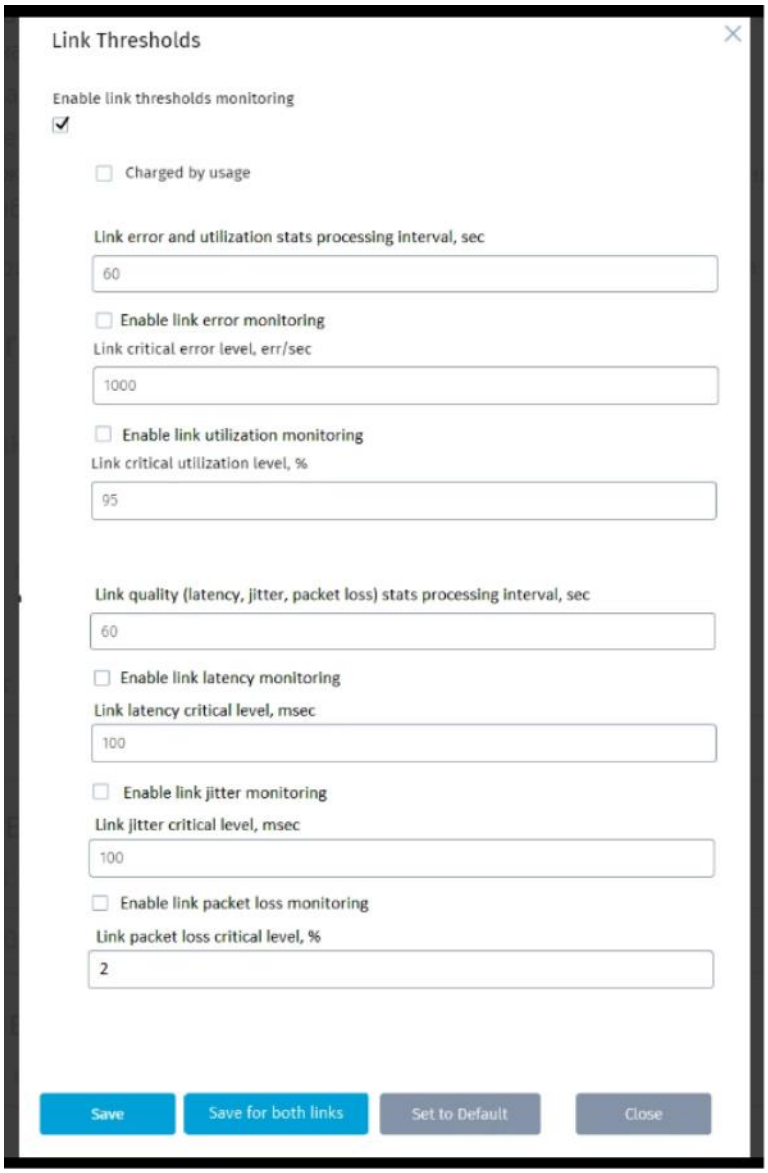

Рис. 24. Параметры мониторинга линков

Вначале необходимо включить мониторинг качества обслуживания на линке – отметить галку «Enable link threshoulds monitoring». Далее настраиваются отдельные параметры мониторинга:

- Charged by usage – безусловная установка нежелательности использования линка или использования его в последнюю очередь, независимо от качества связи;
- Link error and utilization stats processing interval, sec – общий интервал измерения процента ошибок и загрузки линка. Может принимать значения от 30 до 300 сек с шагом 10 сек
- Link critical error level, err/sec - пороговое значение уровня ошибок, от 1 до 1 000 000
- Link critical utilization level, % - пороговое значение загрузки линка в процентах от установленной скорости интерфейса, от 50 до 100 процентов
- Link quality (latency, jitter, packet loss) stats processing interval, sec – общий интервал измерения для параметров Latency, jitter и packet loss. Может принимать значения от 60 до 600 сек с шагом 10 сек
- Link latency critical level, msec – максимальное значение времени задержки при передаче пакетов, от 5 до 1000 мсек

- Link jitter critical level, msec - максимальное значение вариации задержки, от 5 до 1000 мсек
- Link packet loss critical level, % - процент потери пакетов, от 1 до 100 процентов

Скорость интерфейса может не соответствовать реальной полосе туннеля SD-WAN. В этом случае для мониторинга загрузки полосы необходимо задать скорость вручную в настройках SD-WAN контроллера (Switches -> Management -> Interfaces settings).

Результаты мониторинга линков используются далее при создании ограничений (Constraints). При достижении пороговых значений данные линки будут по возможности или строго (в зависимости от настроек) обходиться при построении Auto-TE пути для сервиса.

Окно создания ограничения Constraint приведено на Рис. 25.

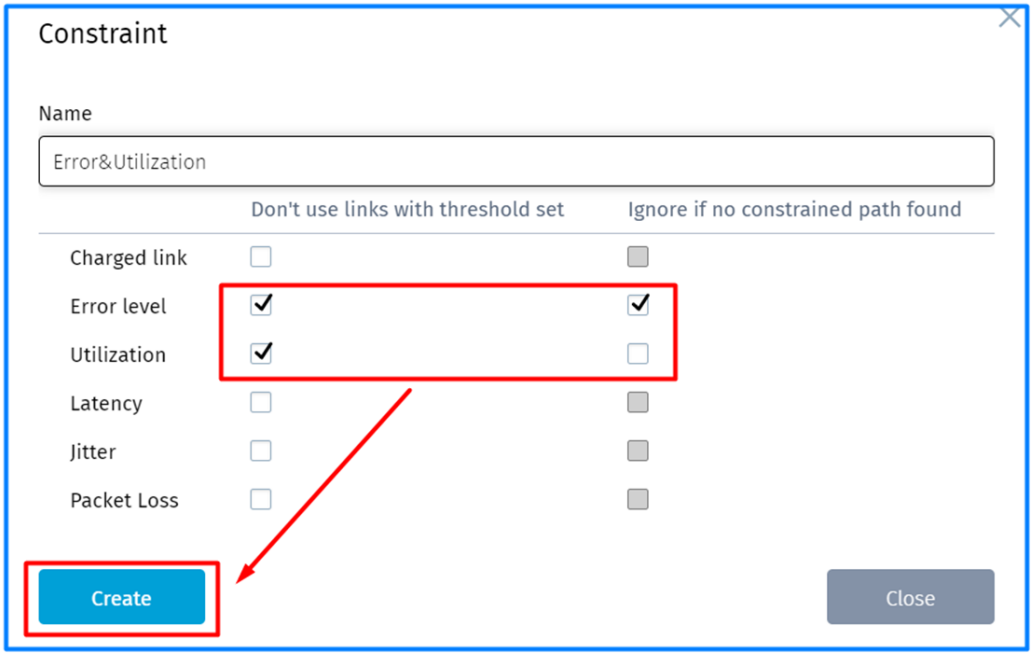

Рис. 25. Создание Constraint

В форме создания Constraint отмечаются параметры, которые должны учитываться при выборе линков. Флаг Ignore справа от каждого параметра определяет, насколько строго необходимо соответствовать заданным параметрам мониторинга в том случае, если удовлетворяющих критериям линков нет в наличии.

В случае, если флаг Ignore установлен, сервис будет работать без соблюдения SLA, если не установлен – трафик передаваться не будет.

Пример созданного ограничения Constraint приведен на Рис. 26.

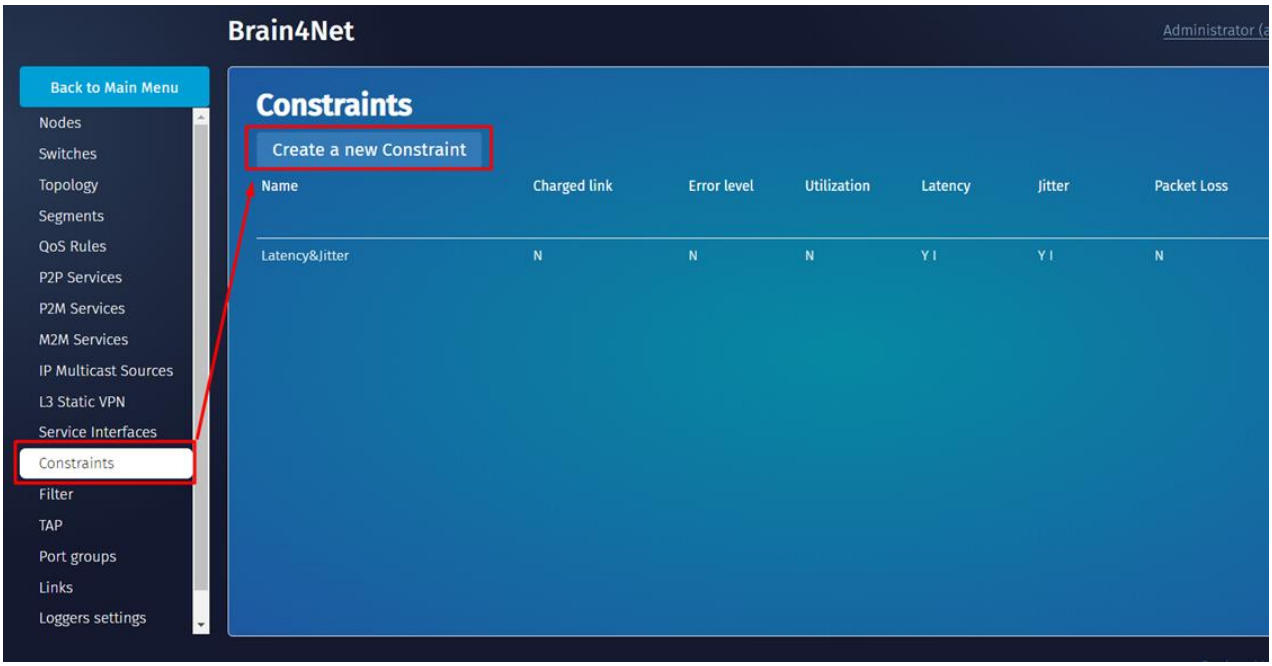

Рис. 26. Пример ограничения Constraint

В таблице присутствует уже созданное ограничение Latency&Jitter. Статус параметров обозначается следующими символами:

- Y - параметр выбран по флагу столбца "Don't use links with threshold set" и не выбран по "Ignore if no constrained path found". При достижении порогового значения по этому параметру линк не будет использоваться.
- Y I - параметр выбран по флагам столбцов "Don't use links with threshold set" и "Ignore if no constrained path found". При достижении порогового значения по этому параметру и отсутствии альтернативных линков данный линк будет использоваться.
- N - параметр не выбран по флагам столбцов "Don't use links with threshold set" и "Ignore if no constrained path found. Параметр не учитывается при расчете путей.

При создании сервиса с соблюдением SLA указывается соответствующее ограничение, и путь будет строиться с его учетом (Рис. 27).

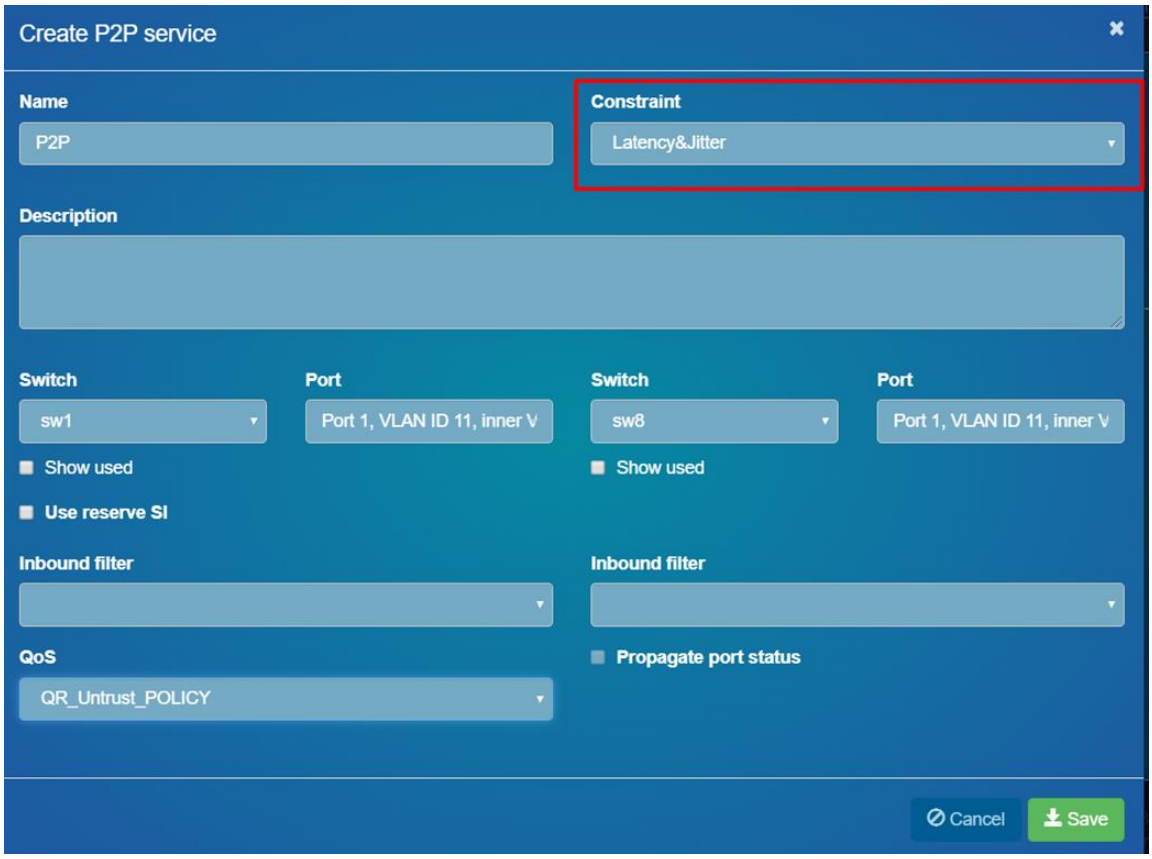

Рис. 27. Применение Constraints при создании сервиса

8.3. Фильтрация трафика

Фильтрация трафика (списки контроля доступа) может использоваться для следующих задач:

- обеспечение безопасности (блокирование избыточного или потенциально опасного трафика и пропуск только легитимного трафика),
- выделение интересующего трафика с целью его зеркалирования,
- обеспечение SLA для определенных приложений.

Порядок создания фильтра:

1. Формируются правила классификации трафика Rules, которые служат для выделения пакетов по значениям заголовков уровней L2 - L4.
2. Затем эти правила используются для формирования фильтра, представляющего собой упорядоченный список правил Rules. Каждому правилу присваивается приоритет и тип действия Permit / Deny , то есть разрешен данный трафик или запрещен.
3. В конце списка Rules задается Default Action Permit / Deny.

8.3.1. Создание правил классификации трафика

Правила классификации трафика позволяют выделить определенный трафик для дальнейшего управления им. Форма для создания правила классификации трафика приведена на Рис. 28.

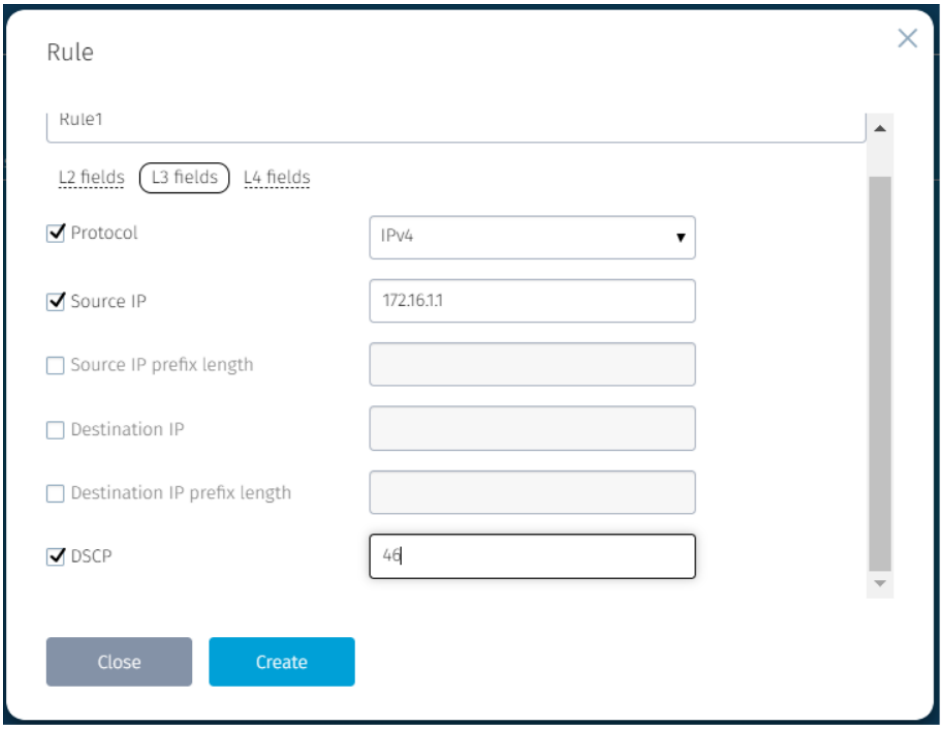

Рис. 28. Создание правила классификации трафика

Перечень полей заголовков, которые можно использовать при создании правила, и их возможных значений приведен в таблице *3*.

Таблица 3. Поля заголовка пакета

Заголовок	**Возможные значения**
Поля заголовка уровня L2	
Outer VLAN id	0-4095
Outer VLAN pcp	0-7
Source MAC	00:00:00:00:00:00 - ff:ff:ff:ff:ff:ff
Source MAC mask	00:00:00:00:00:00 - ff:ff:ff:ff:ff:ff
Destination MAC	00:00:00:00:00:00 - ff:ff:ff:ff:ff:ff
Destination MAC mask	00:00:00:00:00:00 - ff:ff:ff:ff:ff:ff
Ethertype	Выпадающий список: 0x0800 (по умолчанию) 0x86dd 0x0806
Поля заголовка уровня L3	
Protocol (необходимо определить для возможности использования L4 правил)	Выпадающий список: IPv4 (по умолчанию) IPv6
Source IP	Для IPv4: 0.0.0.0 - 255.255.255.255 Для IPv6: 0000:0000:0000:0000:0000:0000:0000:0000 - ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Source IP prefix length	Для IPv4: /0 - /32

	Для IPv6: /0 - /128
Destination IP	Для IPv4: 0.0.0.0 - 255.255.255.255 Для IPv6: 0000:0000:0000:0000:0000:0000:0000:0000 - ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Destination IP prefix length	Для IPv4: /0 - /32 Для IPv6: /0 - /128
DSCP	Выпадающий список
TOS	0 – 255
PKT Mark	1 - 4294967295
Поля заголовка уровня L4	
IP Protocol	Выпадающий список: TCP (по умолчанию) UDP ICMP Other При выборе Other становится активным поле Number для задания значения <0-255>
Source port list	0-65535 Можно задавать список через <,> или диапазон через <->
Destination port list	0-65535 Можно задавать список через <,> или диапазон через <->
ICMP type number	0-255 Может быть указано только 1 значение

Параметр L3 TOS является взаимоисключающим с параметром L3 DSCP - в правиле классификации может использоваться либо один, либо другой параметр.

Правило классификации трафика может быть составным и включать в себя несколько параметров одновременно. В этом случае отдельные условия суммируются друг с другом по логическому AND.

8.3.2. Создание фильтров трафика

Фильтр трафика представляет собой упорядоченную группу правил классификации трафика, в которой каждое правило имеет приоритет и соответствующее действие (разрешить или запретить).

При создании фильтра задаются следующие параметры:

- Name - название фильтра.
- Sequence - порядковый номер добавляемого правила в диапазоне 1-998 (номер 999 у Default action). Правило с меньшим номером имеет больший приоритет.
- Rule - имя правила классификации трафика.
- Action - действие для выбранного правила, разрешить (Permit) или запретить (Deny).
- Add / Delete – добавить правило в список фильтра или удалить.
- Default action - закрывающее правило с наиболее низким приоритетом для остального трафика, не соответствующего правилам из списка.

Пример фильтра трафика приведен на Рис. 29.

Рис. 29. Пример фильтра трафика

При создании сервиса для каждого сервисного интерфейса можно указать ранее созданный фильтр в поле “Inbound Filter”.

8.4. Маршрутизация трафика по приложениям

Фильтры могут использоваться для выделения трафика критичных приложений для его последующей балансировки с соблюдением требований SLA.

Предварительно должны быть выполнены следующие действия:

- Включен режим использования нескольких путей для передачи трафика (multipathing);
- Созданы ограничения Constraints;
- Созданы фильтры трафика;
- Создан стандартный сервис с указанием необходимых сервисных интерфейсов с инкапсуляцией Access, VLAN или Q-in-Q.

Далее необходимо создать специальные сервисные интерфейсы – ACL SI. ACL SI создается поверх обычного (underlay) SI. При создании ACL SI указывается заранее созданный фильтр, по которому будет вестись обработка и отвод трафика в сервис (Рис. 31).

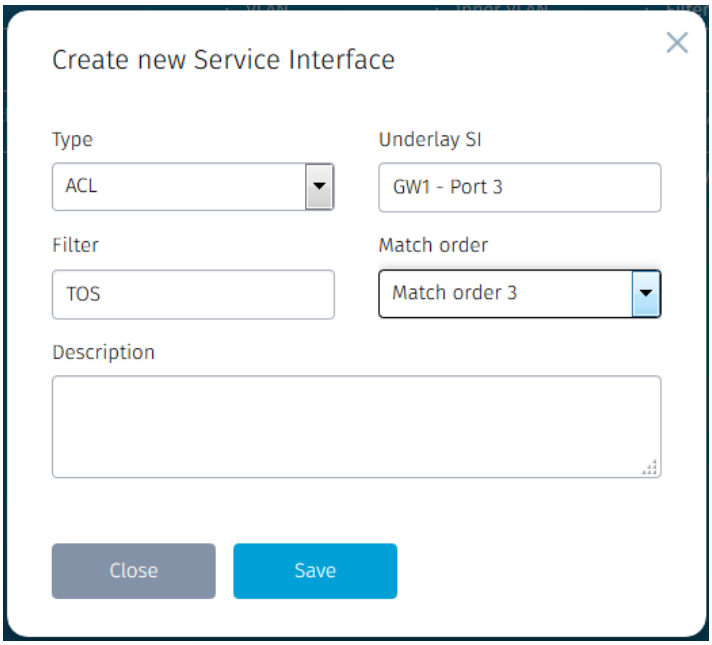

Рис. 30. Создание ACL SI

Match order определяет порядок обработки фильтра. При выборе порядка обработки для ACL SI значение Match order резервируется за данным ACL SI и блокируется для выбора при создании других ACL SI на этом же Underlay SI.

Один и тот же фильтр можно подключать к различным Underlay SI.

Перед удалением Underlay SI сначала необходимо удалить все привязанные к нему ACL SI.

После создания ACL SI для разных типов трафика создаются отдельные сервисы с ACL SI в качестве сервисных интерфейсов и указанием требуемых ограничений Constraints.

На рисунке 31 интерфейс Underlay SI принадлежит к обычному сервису без Constraints, и в него попадает весь трафик, который не отводится в сервисы Blue и Red их фильтрами.

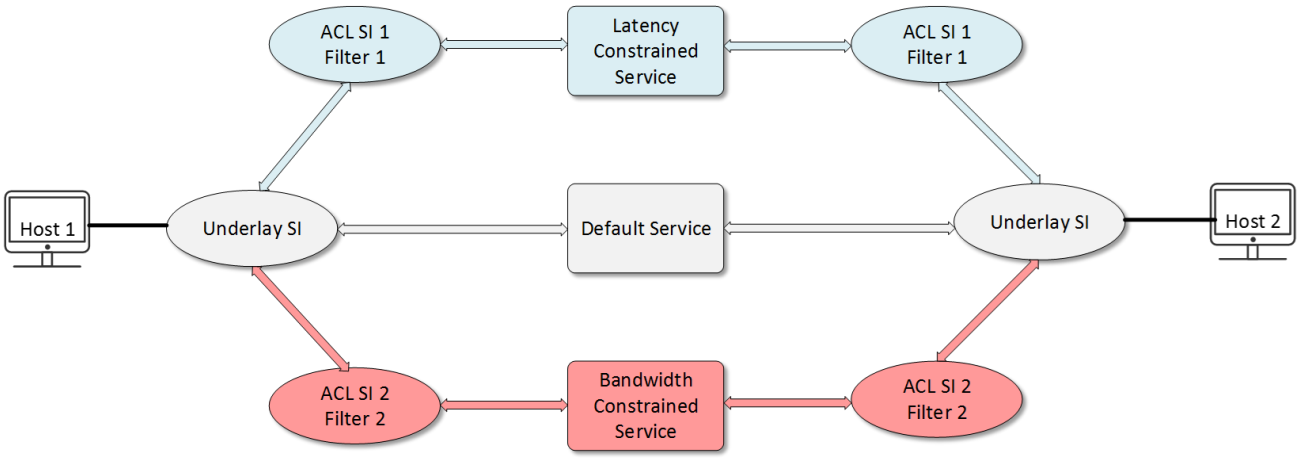

Рис. 31. Маршрутизация трафика по приложениям с соблюдением SLA

Интерфейс ACL SI 1 принадлежит к сервису Blue с Constraint по задержке, в этот сервис с помощью фильтра 1 отводится чувствительный к задержкам трафик.

Интерфейс ACL SI 2 принадлежит к сервису Red с Constraint по доступной полосе пропускания, в этот сервис с помощью фильтра 2 отводится чувствительный к полосе трафик.

9. РЕЗЕРВИРОВАНИЕ И ОТКАЗОУСТОЙЧИВОСТЬ

Архитектура решения и используемые механизмы резервирования обеспечивают работоспособность распределенной сети при возникновении следующих видов сбоев:

- отказ одного из центральных компонентов – оркестратора, SD-WAN контроллера, SD-WAN шлюза
- отказ или перегрузка каналов связи между центральными компонентами при их георезервировании;
- отказ или перегрузка каналов связи между CPE и SD-WAN шлюзами.

9.1. Резервирование центральных компонентов

Схемы резервирования отдельных компонентов решения SD-WAN приведены в таблице 4.

Таблица 4. Схемы резервирования компонентов

Компонент	**Схема резервирования**	**Используемые протоколы**
Оркестратор	N+1	REST
Web-интерфейс оркестратора	N+1	REST
База данных оркестратора (mongodb)	2N+1	MONGODB
SD-WAN контроллер с базой данных	2N+1	OPENFLOW (TLS)
SD-WAN шлюз	N+1	VXLAN (DTLS)

На Рис. 32 приведен пример размещения компонентов решения в географически разнесенных ЦОД. Для компонентов, резервируемых по схеме N+1, развертываются два узла в разных ЦОД. Оба узла находятся в активном состоянии. Выбор, к какому узлу направляются запросы, осуществляется с помощью виртуального IP адреса или службы DNS.

Условные обозначения на схеме:

- www - Web-интерфейс оркестратора
- orc – Оркестратор
- orc-dbs - База данных оркестратора
- ctl – SD-WAN контроллер с базой данных
- GW – SD-WAN шлюз

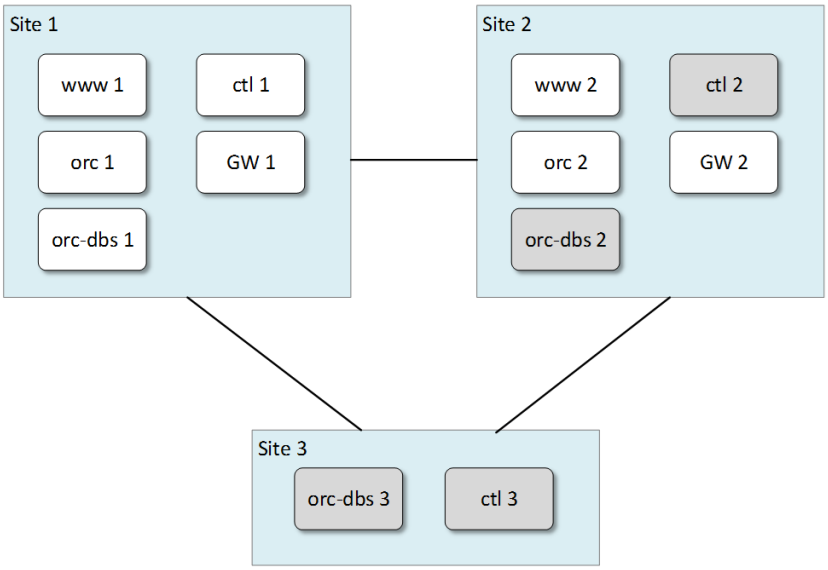

Рис. 32. Размещение компонентов решения в географически разнесенных ЦОД

Компоненты, резервируемые по схеме 2N+1, образуют кластер, в котором один активный узел – мастер, и два узла slave. В целях экономии ресурсов и снижения требований к каналам связи один из узлов может быть назначен арбитром – в этом случае он не будет содержать базу данных и никогда не может быть выбран мастером. Арбитр участвует в голосовании при выборе мастера и обменивается с другими узлами периодическими служебными пакетами (heartbeats).

На рисунках 33 - 36 приведены примеры возможных аварийных ситуаций и ответная реакция системы.

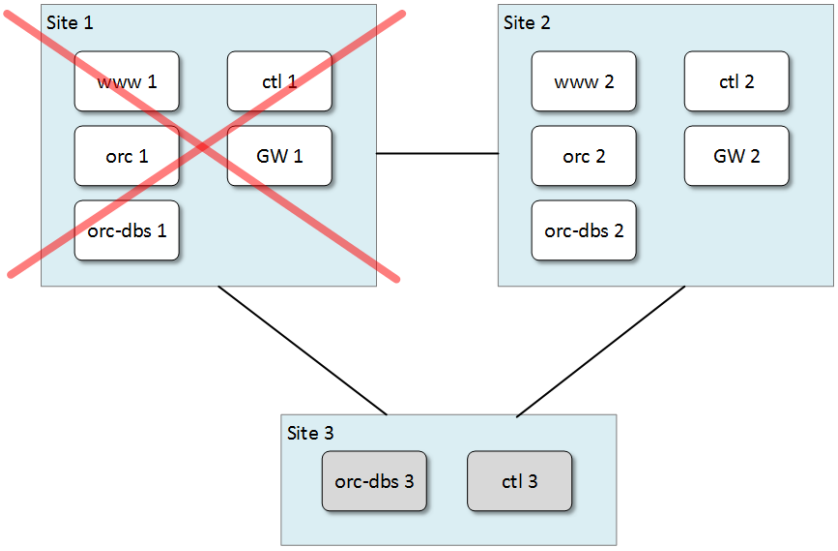

Рис. 33. Выход из строя компонентов системы на Площадке 1

В случае выхода из строя компонентов системы на Площадке 1:

- orc-dbs 2 и orc-dbs арбитр теряют связь с orc-dbs 1 и выбирают нового мастера
- так как orc-dbs арбитр не может стать мастером, orc-dbs 2 становится новым мастером и сообщает клиентам (оркестратору) о своей роли

- ctl 2 и ctl arbiter теряют связь с ctl 1 и выбирают нового мастера
- так как ctl арбитр не может стать мастером - ctl 2 становится новым мастером

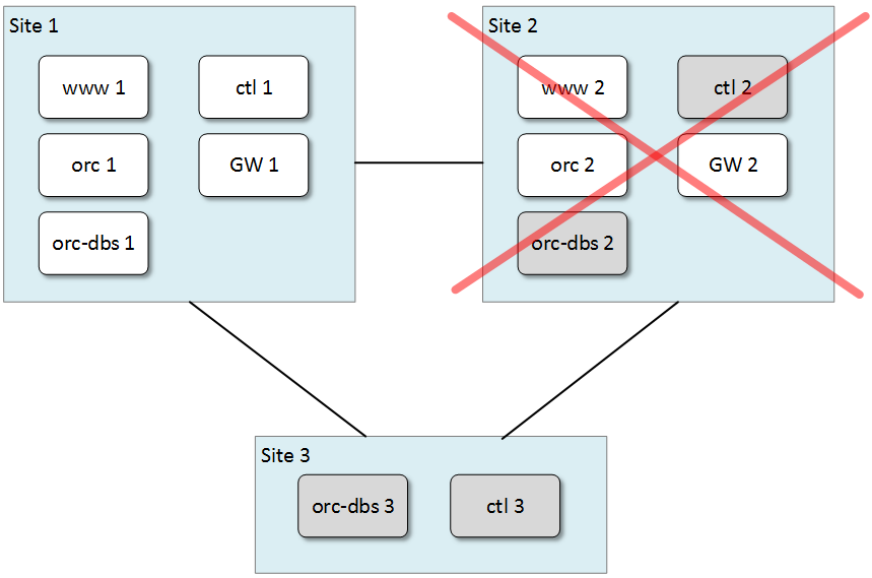

Рис. 34. Выход из строя компонентов системы на Площадке 2

В случае выхода из строя компонентов системы на Площадке 2:

- orc-dbs 1 и orc-dbs арбитр теряют связь с orc-dbs 2 и orc-dbs 1 остается мастером
- ctl 1 и ctl arbiter теряют связь с ctl 2 и ctl 1 остается мастером

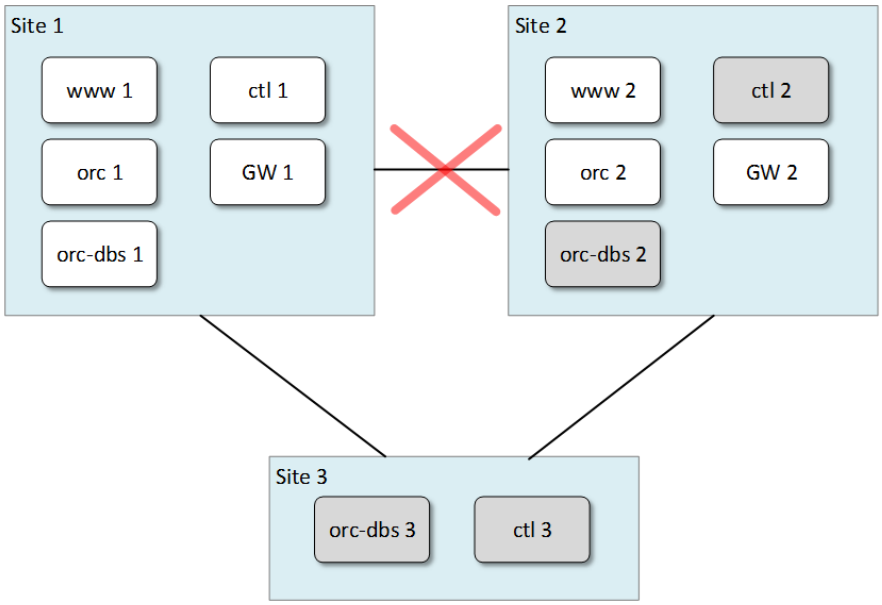

Рис. 35. Разрыв связи между площадками 1 и 2

В случае пропадания связи между площадками 1 и 2:

- orc-dbs 1 и orc-dbs 2 теряют связь друг с другом, и orc-dbs 1 остается мастером, так как orc-dbs арбитр видит, что обе площадки работоспособны
- ctl 1 и ctl 2 теряют связь друг с другом, и ctl 1 остается мастером, так как ctl арбитр видит, что обе площадки работоспособны

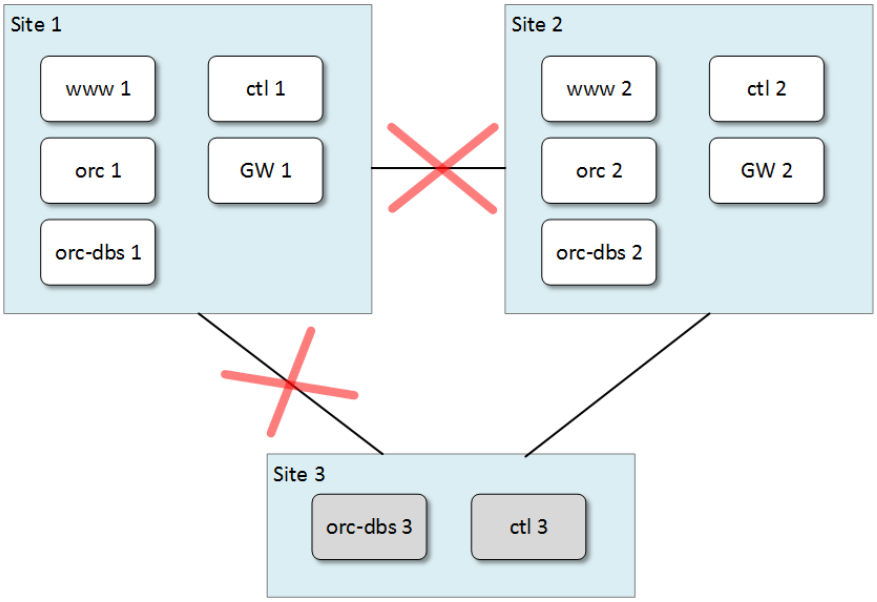

Рис. 36. Разрыв связи между площадками 1 и 2, 1 и 3

В случае пропадания связи между площадкой 1 и остальными площадками:

- orc-dbs 1 и orc-dbs 2 теряют связь друг с другом, и orc-dbs 2 становится новым мастером, так как orc-dbs арбитр видит, что первая площадка также недоступна (то есть ситуация аналогична аварии на площадке 1)
- ctl 1 и ctl 2 теряют связь друг с другом, и ctl 2 становится новым мастером, так как ctl арбитр видит, что первая площадка также недоступна (ситуация аналогична аварии на площадке 1).

9.2. Резервирование каналов связи с CPE

Защита от перерывов связи с CPE обеспечивается одновременным использованием всех доступных каналов (арендуемые каналы, Internet, LTE). Поддерживаются режимы резервирования Active/Active или Active/Standby.

В режиме Active/Active все WAN-порты находятся в активном состоянии и используются для передачи трафика пользователей. SD-WAN контроллер обеспечивает балансировку трафика по нескольким путям (multipathing). Количество путей может составлять от 2 до 16.

Балансировка осуществляется на уровне сессий (flow) с учетом L2-L4 информации. Возможна работа в двух режимах:

- Эквивалентная балансировка - вес каждого пути принимается равным единице. Таким образом достигается равномерное распределение трафика по транспортным путям.
- Неэквивалентная балансировка - трафик распределяется по транспортным путям примерно пропорционально их весу.

В режиме Active/Active CPE остается доступной, пока хотя бы один из каналов связи работоспособен.

В режиме Active/Standby выбираются основной и резервный пути для передачи трафика. SD-WAN контроллер заранее программирует на CPE основной выходной WAN порт и резервный WAN порт на случай отказа основного. Таким образом, при отказе линка не производится переписывание правил коммутации пакетов. CPE сразу начинает отправлять пакеты через резервный порт.

Для всех транспортных сервисов можно указать резервный сервисный интерфейс (Reserve SI), на который переключится трафик сервиса в случае недоступности основного сервисного интерфейса. Обычно основной и резервный сервисные интерфейсы создаются на разных устройствах. Эта функция применяется, например, для резервирования SD-WAN шлюзов. При создании транспортного сервиса в качестве основного сервисного интерфейса (tunnel endpoint) указывается порт на первом шлюзе, и в качестве резервного сервисного интерфейса добавляется порт на втором шлюзе.

На Рис. 37 изображен пример сервиса SD-WAN с двумя SD-WAN шлюзами и тремя CPE, использующими по два WAN порта каждый. Один шлюз является основным, второй - резервным. Каждое из устройств CPE организует по одному туннелю VXLAN до каждого шлюза через каждый порт WAN.

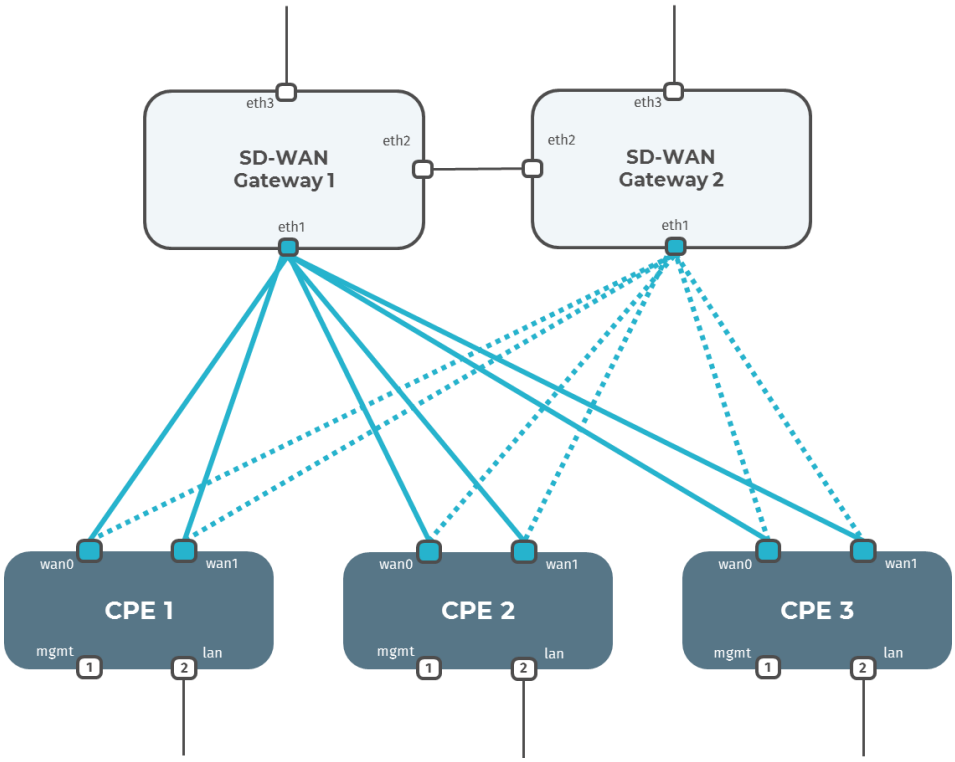

Рис. 37. Резервирование шлюзов и агрегирование каналов

SD-WAN контроллер может быть развернут как один узел или в виде кластера из 3-х узлов.

Пользовательский трафик не проходит через SD-WAN контроллер, поэтому при недоступности контроллера перерыва в передаче данных между CPE и SD-WAN шлюзами не происходит.

9.3. Link Dampening

Основная задача функции Link Dampening - детектирование частых изменений состояния интерфейса (UP-DOWN или наоборот), перемещение всех текущих сервисов, проходящих через интерфейс, на запасные более стабильные пути, и выведение транспортного сегмента, привязанного к этому интерфейсу, из расчета путей для сервисов.

Администратор может активировать функцию Link Dampening и изменить параметры отдельно для каждого линка, если значения по умолчанию не подходят (Рис. 38).

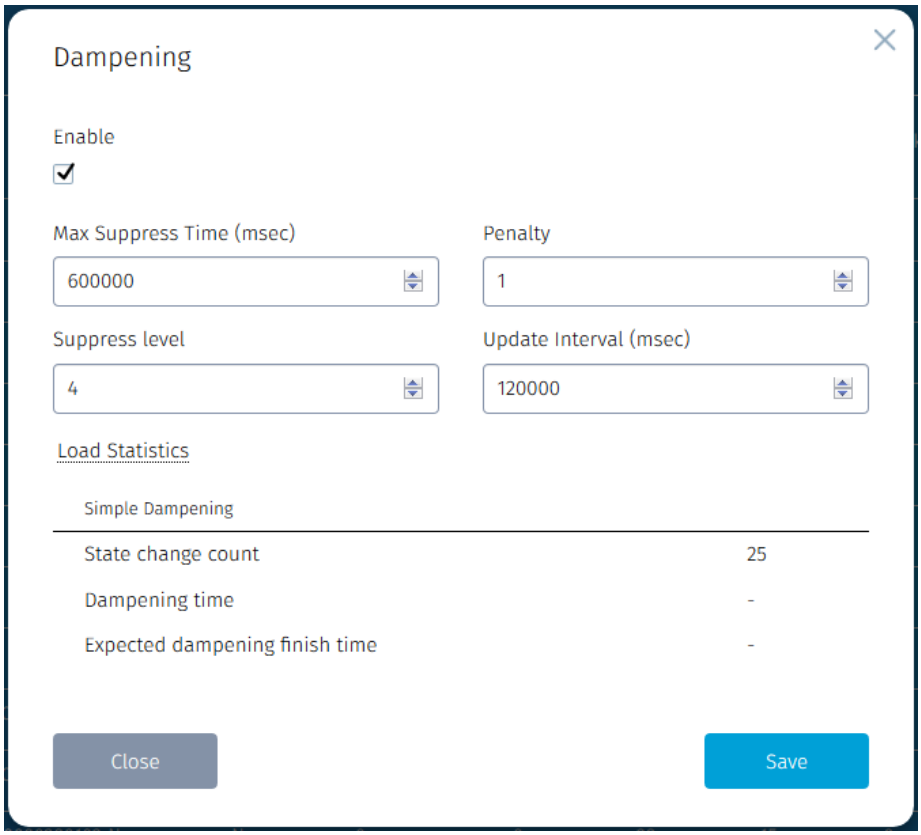

Рис. 38. Настройка Link Dampening для отдельного линка

Значения полей окна “Dampening”:

- Max Suppress Time — Максимальное время, на которое может быть заблокирован интерфейс. По истечении этого времени счетчики сбрасываются;
- Suppress level — Значение Penalty, при котором активируется ограничение доступа к интерфейсу;
- Update Interval - Интервал времени, за которое интерфейс должен набрать Penalty до значения Suppress level.

По умолчанию, возврат интерфейса и связанного с ним транспортного сегмента в работу происходит, если в течение 10 минут интерфейс не испытывает изменения состояния.

10. ТРЕБОВАНИЯ К АППАРАТНОМУ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ

10.1. Требования к аппаратному обеспечению

Аппаратные ресурсы, необходимые для развертывания решения B4N SD-WAN, включают в себя серверы (или виртуальные машины) для установки платформы B4N Service Platform, системы мониторинга Zabbix, SD-WAN контроллеров и шлюзов.

Сервис SD-WAN может быть развернут как VNF или PNF.

Установка в виде VNF требует виртуальной инфраструктуры под управлением OpenStack. Экземпляры VNF SD-WAN для тенантов развертываются на узлах OpenStack Compute Node.

Если сервис SD-WAN развертывается как PNF, виртуальные машины SD-WAN контроллера и SD-WAN шлюзов устанавливаются вручную.

Требования к аппаратным ресурсам в зависимости от количества управляемых CPE приведены в табл. 5.

Таблица 5. Требования к аппаратным ресурсам для решения B4N SD-WAN

Назначение	**Кол-во ядер процессора**	**Оперативная память, Гбайт**	**Дисковое пространство, Гбайт**	**Сетевые адаптеры**	**Кол-во серверов/VM**
Серверы/VM для установки платформы B4N Service Platform					
Оркестратор					
до 500 CPE	12	24	1000	2x10G, 2x1GE	3
до 1000 CPE	12	24	1000	2x10G, 2x1GE	3
до 10000 CPE	16	40	1500	2x10G, 2x1GE	3
SDN Controller (если используется VNF SD-WAN)					
до 500 CPE	8	16	150	2x10G, 2x1GE	3
до 1000 CPE	8	24	150	2x10G, 2x1GE	3
до 10000 CPE	12	32	300	2x10G, 2x1GE	3
VNFM					
до 500 CPE	1	2	40	2x10G, 2x1GE	2
до 1000 CPE	1	4	40	2x10G, 2x1GE	2
до 10000 CPE	8	16	500	2x10G, 2x1GE	2

Продолжение таблицы 5. Требования к аппаратным ресурсам для решения B4N SD-WAN

Назначение	**Кол-во ядер**	**Оперативная**	**Дисковое**	**Сетевые**	**Кол-во**

	процессора	память, Гбайт	пространство, Гбайт	адаптеры	серверов/VM
Серверы/VM мониторинга					
Zabbix Server					
до 500 CPE	4	8	150	2x10G, 2x1GE	2
до 1000 CPE	4	8	150	2x10G, 2x1GE	2
до 10000 CPE	18	34	1200	2x10G, 2x1GE	2
Zabbix Proxy					
до 500 CPE	1	2	20	2x10G, 2x1GE	2
до 1000 CPE	4	8	50	2x10G, 2x1GE	2
до 10000 CPE	8	16	50	2x10G, 2x1GE	2
Сервис SD-WAN					
SD-WAN Controller	8	16	150	1x10G, 2x1GE	3
SD-WAN Шлюз	8	16	40	2x10G, 2x1GE	2

При планировании ресурсов для сервиса SD-WAN возможна переподписка. Коэффициент переподписки зависит от количества CPE на 1 инстанс, частоты изменений в сети, скорости передачи трафика и размера передаваемых пакетов.

В таблице указано количество серверов и аппаратных ресурсов с учетом резервирования для обеспечения высокой доступности решения. В лабораторных условиях возможна установка без резервирования, когда каждый компонент устанавливается в одном экземпляре.

10.2. Требования к программному обеспечению

Поддерживаемые операционные системы (x64):

- Debian версии 8.1 и выше
- Ubuntu версии 14.04 и выше
- CentOS версии 7.1 и выше
- RedHat версии 7.1 и выше
- SUSE версии 12.4 и выше

Для установки системы требуется Docker версии 1.5 или выше.

10.3. Требования к CPE

В качестве CPE могут быть использованы устройства любых производителей, удовлетворяющие требованиям:

- Стандартная архитектура x86 или ARM
- Количество ядер процессора - не менее 2
- Объем оперативной памяти - не менее 128 Мбайт
- Количество портов LAN - 1 или более
- Количество портов WAN - 2 или более

В таблице 6 в качестве примера приведены некоторые из протестированных моделей CPE.

Таблица 6. Протестированные модели CPE

Модель	**Процессор**	**Cores**	**RAM**	**Disk / Flash**	**Ethernet**	**LTE**	**WiFi**
Булат BM10-2xLTE-HP	MediaTek MT7621AT (880 MHz)	2	512 MB	16 Mb	5x1G RJ45	2xEC25 LTE modem	2.4 + 5 Ghz
Булат BM10-2xLTE	MediaTek MT7620A (MIPS 24KEc) 580MHz	1	128Mb DDR3	16 Mb	5 x 10/100 RJ45	2xEC25 LTE modem	2.4Ghz (802.11bgn)
Depo 2121	Intel(R) Atom(TM) CPU C2358 @ 1.74GHz	2	8GB	55 GB	6 x 10/100/1000 RJ45		

Для сценария uCPE, когда планируется запуск виртуальных сетевых функций на CPE, необходимо предусмотреть дополнительные вычислительные ресурсы в соответствии с требованиями VNF. В качестве uCPE поддерживаются устройства с x86 архитектурой.

Протестированные модели uCPE приведены в табл. 7.

Таблица 7. Протестированные модели uCPE

Модель uCPE	Булат CPE C3000	DEPO Stream 1060CX
Пропускная способность		
Процессор	Intel® Atom® processor C3758 (8-Core, 2.2GHz, 16MB	Intel® Celeron® J1900 (4-Core, 2.0GHz, 2MB)
RAM	8GB DDR4 ECC	2GB DDR3L SO-DIMM 1.35V
Сетевые порты	2 x SFP, 6 x Gbe	6 x 1Gbe RJ45 (Intel i211)

Flash	-	1GB Compact Flash SLC
SSD	128GB SSD	200GB SSD

11. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ

Решение B4N SD-WAN основано на применении технологий SDN и NFV в распределенных сетях и состоит из нескольких уровней - уровень передачи данных (data plane), уровень управления сетью (control plane) и уровень оркестрации. Безопасность решения в целом определяется безопасностью каждого уровня в отдельности, а также взаимосвязей между ними.

На всех уровнях обеспечивается:

- Аутентификация и авторизация пользователей;
- Использование безопасных протоколов управления;
- Шифрование управляющего трафика

Для безопасности клиентов применяется шифрование данных и изоляция трафика в рамках отдельных тенантов и сетевых сервисов. Обеспечивается безопасное подключение CPE.

11.1. Аутентификация и авторизация

Управление платформой осуществляется из графического интерфейса оркестратора или с помощью API. Остальные компоненты решения (кроме CPE) не имеют графического интерфейса.

Для получения доступа к системе через GUI оркестратора или API необходимо авторизоваться.

Информация о пользователях и группах может храниться в локальной базе данных или импортироваться из внешней системы LDAP. Для возможности интеграции с внешними службами каталогов поддерживаются протоколы LDAP и LDAPS.

При добавлении сервера LDAP указывается путь, где искать учетные записи пользователей, и учетная запись с правами read-only, которую оркестратор будет использовать для поиска.

Для импортированных пользователей и групп назначается роль в системе и при необходимости осуществляется привязка к тенанту.

Группы и учетные записи локальных пользователей создаются в графическом интерфейсе оркестратора (рис. 39).

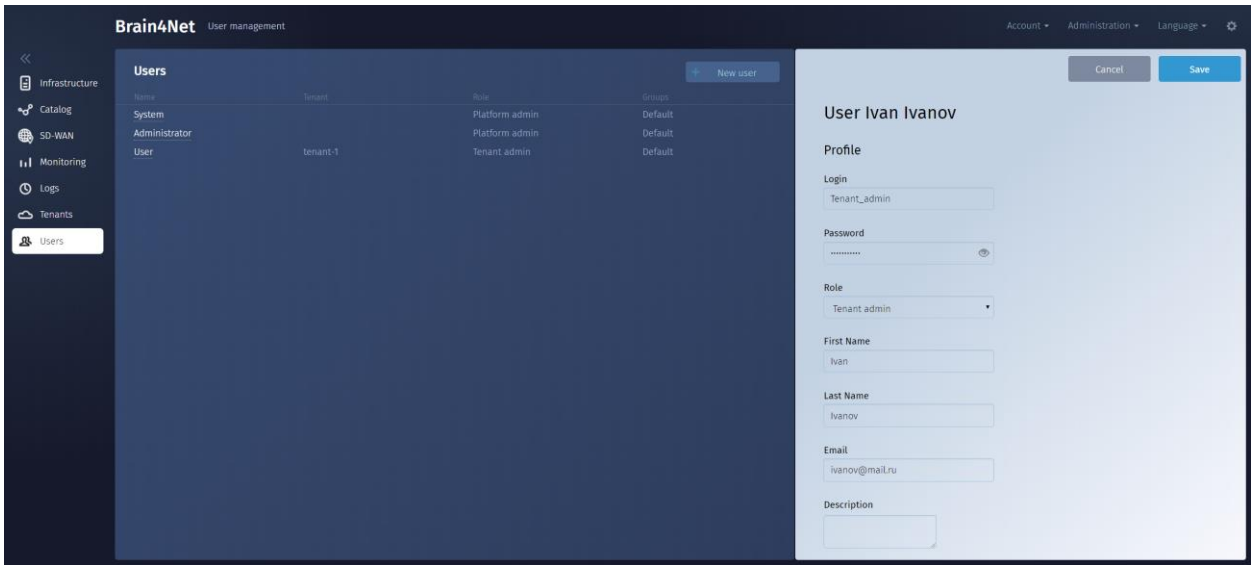

Рис. 39. Добавление учетной записи пользователя

Учетные записи пользователей сразу после их создания являются неактивными. Администратор платформы должен разблокировать учетную запись, чтобы пользователь мог войти в систему.

11.2. Использование безопасных протоколов управления

Взаимодействие с системой (через графический интерфейс управления или API) рекомендуется осуществлять с использованием протокола HTTPS. Могут использоваться собственные сертификаты, которые необходимо заранее загрузить в систему, или автоматически сгенерированные самоподписанные сертификаты.

Список протоколов, используемых для передачи управляющего трафика между компонентами системы, приведен в табл. 8.

Таблица 8. Используемые протоколы для передачи трафика управления

Взаимодействующие компоненты	**Протокол**	**Дополнительное обеспечение безопасности**
Оркестратор - контроллер	gRPC	TLS для аутентификации и шифрования трафика между клиентом и сервером
Оркестратор - CPE	HTTPS	
Контроллер - CPE	OpenFlow 1.3.4	TLS для аутентификации и шифрования трафика между контроллером и CPE

Шифрование пользовательского трафика внутри туннелей VXLAN осуществляется по протоколу DTLS.

11.3. Безопасное подключение CPE и контроль конфигурации

Для идентификации CPE в момент установки и авторизации регистрации используются следующие механизмы:

- DPID устройства, заранее сконфигурированный в CPE
- механизм отложенной регистрации, предусматривающий вмешательство администратора для активации подключенного устройства
- возможен механизм двухфакторной авторизации, предусматривающий передачу клиенту ключа по стороннему каналу и ожиданию корректного ответа со стороны CPE

В процессе регистрации CPE отсылает оркестратору свой уникальный идентификатор - DPID (datapath id). При формировании DPID могут использоваться различные идентификаторы устройства, например, MAC адрес или серийный номер.

Оркестратор сравнивает DPID, полученный от CPE, с DPID устройств в инвентаризационной базе. Если такой DPID существует, оркестратор возвращает CPE информацию, необходимую для подключения к сети (IP адреса SD-WAN контроллера и шлюзов). Если переданный CPE идентификатор отсутствует в инвентаризационной базе, устройство отображается в CPE Inventory со статусом Unknown и в сеть SD-WAN не включается.

Механизм отложенной регистрации позволяет задать, в каком состоянии будет находиться устройство после успешной регистрации - активном или заблокированном. Заблокированное устройство администратор должен активировать вручную после получения дополнительного подтверждения, что именно это оборудование установлено на площадке заказчика.

После активации CPE и подключения к сети управления (Management-P2M) VNF Manager загружает на устройство его конфигурацию. Локальное изменение конфигурации может быть разрешено или запрещено по выбору администратора.

Перед удалением CPE из сети администратор имеет возможность очистить конфигурацию устройства.

11.4. Использование VNF с функциональностью защиты данных

Дополнительный уровень безопасности может быть обеспечен с помощью виртуальных сетевых функций, развернутых в ЦОД сервис-провайдера. Трафик от CPE может направляться в VNF, например, межсетевого экрана или Proxy-сервера. Альтернативный вариант, когда VNF запускаются непосредственно на CPE, также возможен, если CPE содержит достаточное количество аппаратных ресурсов.

Перечень доступных виртуализированных функций может включать в себя Next-Generation Firewall (NGFW), защиту от атак DDOS (Distributed Denial of Service), систему обнаружения и предотвращения вторжений (IPS/IDS), антивирус, антиспам, средства фильтрации URL и Web-контента, защиту от утечек информации (Data Loss Prevention — DLP), Secure Web Proxy и другие продукты.

12. СЦЕНАРИИ ПРИМЕНЕНИЯ

Топология сети SD-WAN определяется выбором транспортных сервисов в шаблоне SD-WAN Instance Template.

12.1. Организация топологии Hub-and-Spoke без возможности связи между удаленными офисами

Топология Hub-and-Spoke считается классической и является наиболее распространенной при создании распределенных сетей.

В данной топологии удаленные площадки подключаются к центральному офису и не могут напрямую связываться друг с другом (рис. 40). Такие сети проще в проектировании и обслуживании, все необходимые сервисы и приложения размещаются в центральном ЦОД.

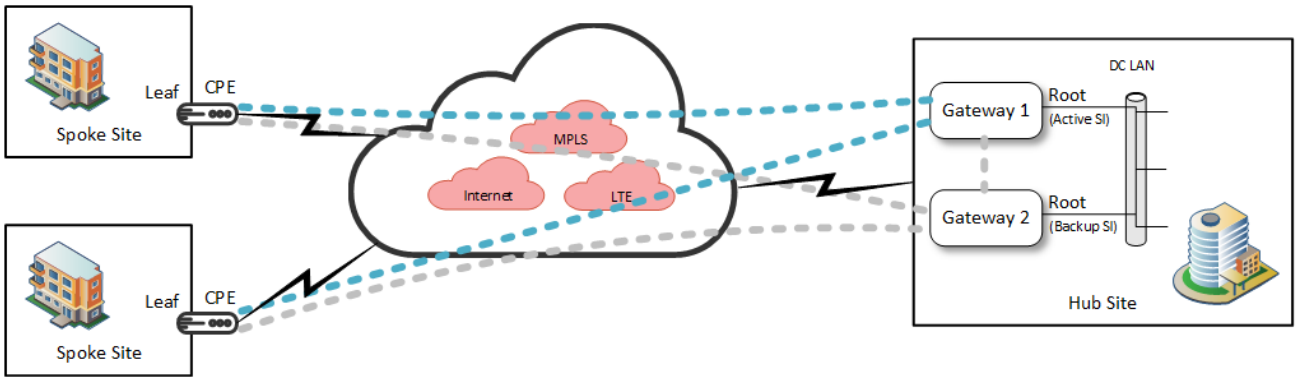

Рис. 40. Топология Hub-and-Spoke с сервисом P2M

В шаблоне SD-WAN Instance Template для организации связи между офисами создается L2 сервис типа P2M (Point-to-Multipoint, или E-Tree). В качестве конечных точек сервиса указываются соответствующие порты на SD-WAN шлюзах 1 и 2. Этим конечным точкам (сервисным интерфейсам) будет назначена роль Root. CPE, регистрирующиеся на оркестраторе, будут автоматически включаться в сервис с ролью Leaf. CPE могут находиться за NAT (PAT).

В данном сценарии передача трафика напрямую между CPE, в том числе через шлюз в качестве транзитного узла, запрещена. В соответствии с выбранными параметрами QoS полоса пропускания может быть ограничена как в целом для CPE, так и для определенных классов трафика.

12.2. Организация топологии Hub-and-Spoke с возможностью связи между офисами через центральный офис

В этом сценарии все офисы могут связываться друг с другом, но только через центральный офис (Hub). Пример топологии показан на рис. 41. CPE могут находиться за NAT (PAT).

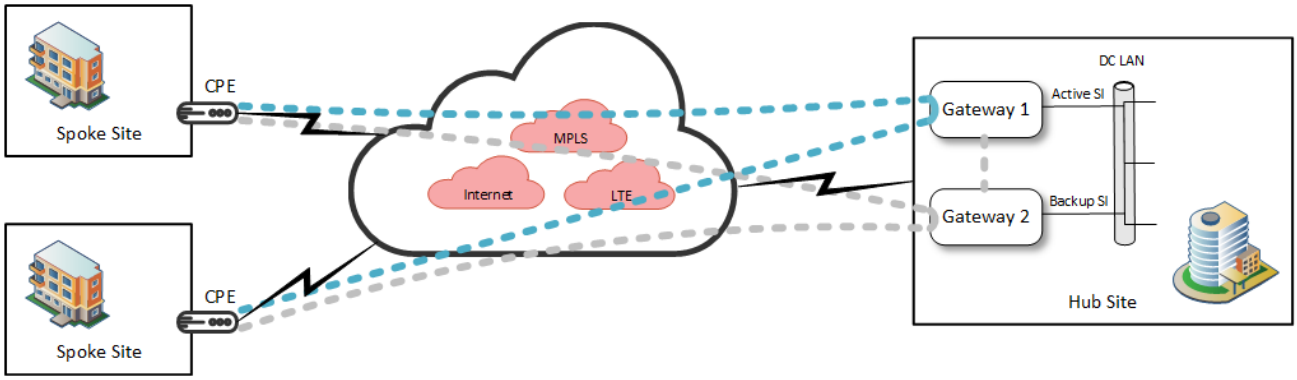

Рис. 41. Топология Hub-and-Spoke с сервисом M2M

В шаблоне Customer Template для организации связи между офисами создается L2 сервис типа M2M (Multipoint-to-Multipoint, или E-LAN). В качестве конечных точек сервиса указываются соответствующие порты на SD-WAN шлюзах 1 и 2. CPE, регистрирующиеся на оркестраторе, будут автоматически включаться в сервис.

В соответствии с выбранными параметрами QoS полоса пропускания может быть ограничена как в целом для CPE, так и для определенных классов трафика.

12.3. Организация топологии Hub-and-Spoke с возможностью связи между офисами через сервисную цепочку в ЦОД

Данный сценарий может применяться, если весь трафик между площадками должен проходить через виртуальные сетевые функции, развернутые в ЦОД (рис. 42). Это позволяет обеспечить безопасность межсетевого обмена, осуществлять мониторинг и инспектирование всех или выбранных пакетов, кэшировать данные и выполнять другие задачи, используя централизованные ресурсы.

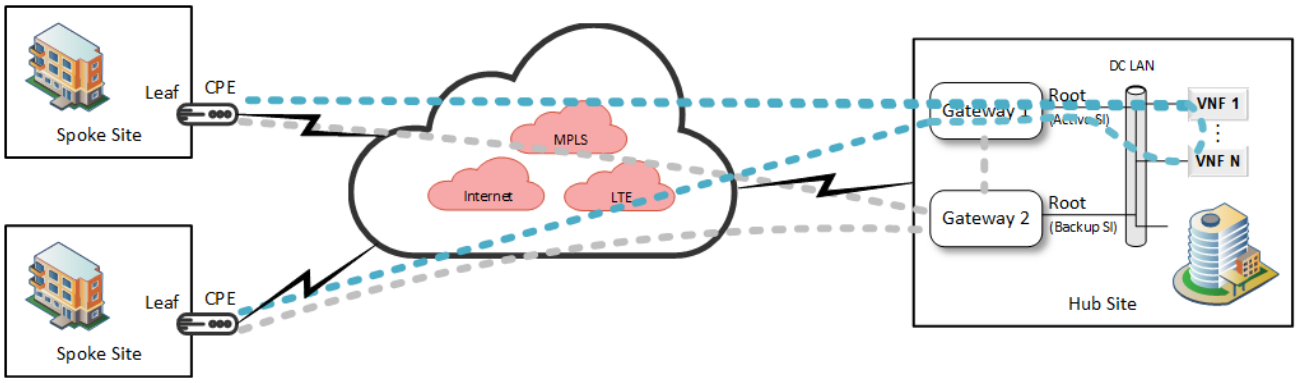

Рис. 42. Топология Hub-and-Spoke с сервисом M2M

В шаблоне SD-WAN Instance Template создается L2 сервис типа P2M (Point-to-Multipoint, или E-Tree).

Для реализации этого сценария необходимо, чтобы сетевой сервис SD-WAN, развернутый для тенанта, содержал в цепочке все необходимые VNF.

12.4. Организация услуги L3 VPN

Сервис L3 VPN со статической маршрутизацией позволяет предоставить клиентам услугу создания маршрутизируемой сети между непосредственно подключенными сетями клиента с возможностью добавления статических маршрутов.

Если в сети необходимо использовать динамическую маршрутизацию, то реализовать такое требование можно, создав L2 P2M транспортный сервис и включив в сервисную цепочку SD-WAN виртуальную сетевую функцию маршрутизатора.

13. ЗАКЛЮЧЕНИЕ

Деятельность современных распределенных компаний в большой степени зависит от надежности и производительности корпоративных сетей передачи данных. В то же время важным бизнес-требованием является снижение стоимости и операционных расходов, связанных с поддержанием работоспособности и развитием сети, при сохранении ее высокой надежности и масштабируемости.

Традиционный подход к созданию распределенных сетей не позволяет в полной мере соответствовать изменяющимся требованиям. К недостаткам классической архитектуры, использующей, как правило, MPLS-транспорт с резервными каналами через Интернет или LTE, можно отнести недостаточную полосу пропускания и ее высокую стоимость, сложность обслуживания, значительные временные затраты при добавлении в сеть новых узлов или изменении политик, отсутствие инструментов для автоматизации управления сетью.

Технология SD-WAN разработана с целью обойти эти ограничения. Решение B4N SD-WAN позволит существенно ускорить процесс подключения новых офисов и снизить сопутствующие затраты. За счет одновременного использования всех доступных каналов связи оптимизируются расходы на каналы без потери качества соединения и снижения эффективной полосы пропускания.

Согласно прогнозу компании Gartner, Inc, к концу 2023 года в более чем 90% проектов модернизации инфраструктуры распределенных сетей будут использоваться технологии SD-WAN и vCPE.