



26.11.2024

Версия документа:
2.3.1.0

Kaspersky SD-WAN

Передача трафика через SD-WAN для
сценариев KICS

kaspersky активируй
будущее

Центр экспертизы
по корпоративным решениям

Изменения

Дата	Изменения
26.11.2024	Первая версия документа

Содержание

1. Описание схемы демонстрационного стенда Kaspersky SD-WAN	4
2. Настройка передачи SPAN через SD-WAN.....	6
2.1. Перевести сетевые интерфейсы eth2 в режим L2 на устройствах CPE-1 и CPE-4.....	6
2.2. Создать сервисные интерфейсы на CPE-1 и CPE-4	7
2.3. Создать транспортный сервис P2P для передачи SPAN.....	9
3. Настройка TAP для зеркалирования трафика от транспортных сервисов	10
3.1. Настроить сетевые интерфейсы на CPE-2 и CPE-3	10
3.2. Настроить BGP на CPE-2 и CPE-3	12
3.3. Создать сервисные интерфейсы на CPE-2 и CPE-3	15
3.4. Создать транспортный сервис M2M.....	16
3.5. Создать TAP для зеркалирования трафика на CPE-4	17
4. Приложение А. Настройка передачи тегированного трафика через SD-WAN	20
4.1. Перевести интерфейсы eth3 в режим L2 на CPE-2 и CPE-3.	21
4.2. Создать сервисные интерфейсы на CPE-2 и CPE-3	22
4.3. Создать транспортный сервис P2P	23

1. Описание схемы демонстрационного стенда Kaspersky SD-WAN

В этом документе описывается настройка решения Kaspersky SD-WAN для передачи SPAN-трафика на KICS, схема демонстрационного стенда представлена на рисунке 1.

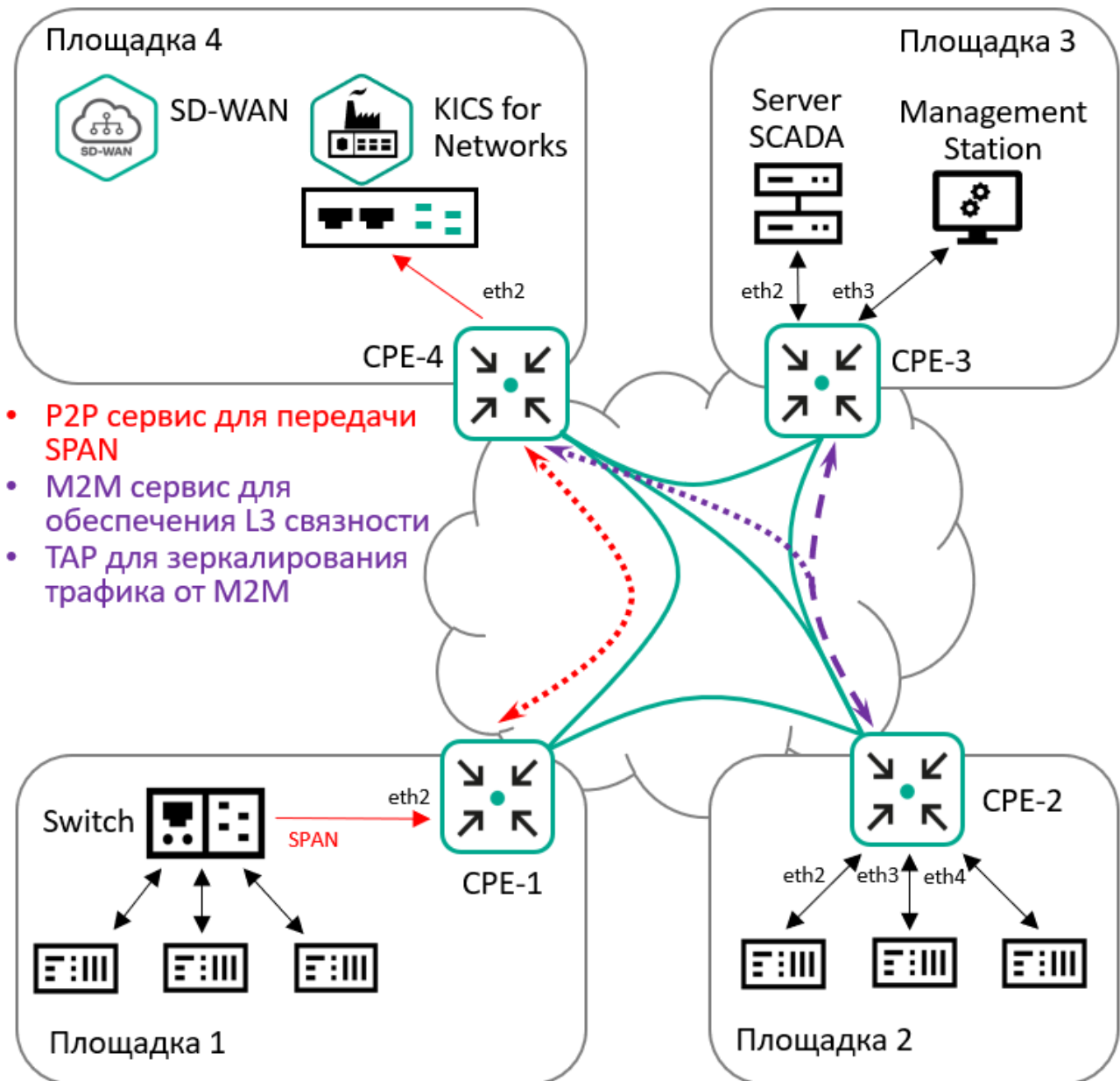


Рисунок 1 – Схема демонстрационного стенда

На схеме представлены четыре площадки с устройствами CPE-1, CPE-2, CPE-3 и CPE-4.

На площадке 1 пользовательские устройства подключены к внешнему коммутатору, который отправляет копию трафика на устройство CPE-1.

На площадках 2 и 3 пользовательские устройства подключены непосредственно к устройствам CPE-2 и CPE-3.

На площадке 4 расположен сервер KICS, на который отправляется трафик от удаленных устройств CPE для анализа.

Устройство CPE-1 получает копию сетевого трафика SPAN от внешнего коммутатора на сетевой интерфейс eth2. На устройствах CPE-1 и CPE-4 сетевые интерфейсы eth2 переведены в режим L2 для прямой работы в Open vSwitch, что позволяет настроить сервисные интерфейсы непосредственно на физических портах. На сетевом интерфейсе eth2 устройства CPE-1 создан сервисный интерфейс с классификацией Access, который принимает весь трафик от коммутатора. На сетевом интерфейсе eth2 устройства CPE-4 создан сервисный интерфейс с классификацией VLAN с тегом 2 для передачи SPAN-трафика на KICS с тегом 2, что позволяет отличать SPAN-трафик с различных площадок. Для отправки трафика от устройства CPE-1 до CPE-4 создан транспортный сервис P2P.

Устройства CPE-2 и CPE-3 выступают в качестве L3-шлюза по умолчанию для локальных сегментов сети и маршрутизируют трафик на удаленные площадки. Локальные сегменты подключены к сетевым интерфейсам eth2-4 на устройствах CPE-1 и CPE-2. Сетевое взаимодействие между площадками осуществляется посредством транспортного сервиса M2M и с использованием протокола BGP для динамической маршрутизации. Для передачи IP-трафика между сегментами за устройствами CPE-2 и CPE-3 настроен мост, объединяющий сетевые интерфейсы eth2-4 и выступающий в качестве шлюза по умолчанию для локального сегмента сети. Для обмена маршрутной информацией с использованием BGP используется сетевой интерфейс overlay.

Для отправки копии трафика с транспортного сервиса M2M между устройствами CPE-2 и CPE-3, на сетевом интерфейсе eth2 устройства CPE-4 создан сервисный интерфейс с классификацией VLAN с тегом 3. Создан TAP-сервис от M2M-сервиса до сервисного интерфейса на устройстве CPE-4 с точкой назначения зеркалирования на сервисном интерфейсе устройства CPE-4.

В следующих секциях описана настройка Kaspersky SD-WAN для осуществления сценария.

Также дополнительно описан вариант настройки устройств CPE-2 и CPE-3 для передачи тегированного L2-трафика между площадками.

2. Настройка передачи SPAN через SD-WAN

2.1. Перевести сетевые интерфейсы eth2 в режим L2 на устройствах CPE-1 и CPE-4.

Требуется перевести сетевые интерфейсы **eth2** на устройствах **CPE-1** и **CPE-4** в режим **L2**.

Открыть шаблон **CPE-1** в меню **SD-WAN** → **CPE templates**

Выбрать вкладку **Network**.

CPE-1-template					
Information Multipathing Deactivation Encryption Scripts SD-WAN Topology Network BGP VRF OSPF Routing filters BFD Static routes Multicast VRRP CFM Monitoring					
+ Network interface					
Alias	Interface name	Protocol	IP/mask	Enable automatically	
overlay	overlay	Static IPv4 address	IP: 172.16.1.1 Mask: 255.255.255.0	Yes	Edit Delete Disable
sdwan0	eth0	DHCP client		Yes	Edit Delete Disable
sdwan1		QMI			Edit Delete Disable

Нажать на кнопку **+ Network interface** и добавить сетевой интерфейс **eth2** со следующими параметрами:

- **Alias** : eth2
- **Interface name** : eth2
- **Protocol** : None
- Установить флажок **L2 mode** для перевода сетевого интерфейса в режим **L2**
- Установить флажок **Enable automatically**

New network interface

Alias ?

eth2

Interface name ?

eth2

Protocol

None

☒ L2 mode ?

OpenFlow port ?

12

⚠ To enable L2 mode, you must create a service interface mapped to the specified OpenFlow port in the controller configuration menu

Settings

☒ Enable automatically ?

Override MAC ?

Override MTU ?

Close

Create

Повторить для шаблона **CPE-4**.

2.2. Создать сервисные интерфейсы на CPE-1 и CPE-4

Перейти в меню SD-WAN → Infrastructure → Контроллер SD-WAN → Configuration menu → Service Interfaces.

Service interfaces

Switch: CPE [CPE-1: 80001C57D815D7] Port: All **Create service interface**

Port	Type	Description	VLAN	Inner VLAN	Filter	Name	Management
2	Access					SI://CPE [CPE-1: 80001C57D815D727]/p:2	Management

Выбрать **CPE-1**, затем нажать на кнопку **Create service interface**.

Задать параметры сервисного интерфейса:

- **Port** : eth2
- **Type** : **Access** (на сервисном интерфейсе будут приниматься как тегированные, так и нетегированные кадры)

Нажать на кнопку **Create**.

Note: На порту нельзя одновременно настроить сервисные интерфейсы с классификацией Access и VLAN/QinQ.

New service interface

Port: 12 (eth2)

Type: Access

Description:

Close Create

Повторить для **CPE-4** с параметрами:

- **Port** : eth2
- **Type** : VLAN
- **VLAN ID** : 2

New service interface

Port

12 (eth2)

Type

VLAN

VLAN ID

2

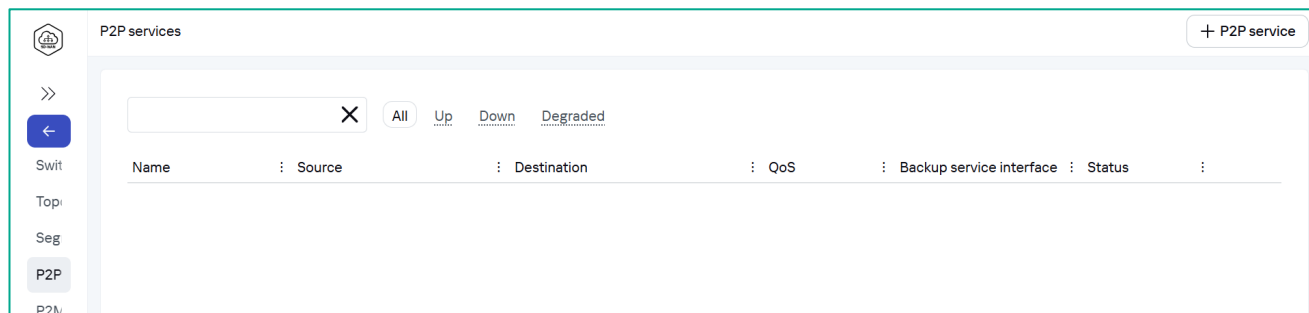
Description

Close

Create

2.3. Создать транспортный сервис P2P для передачи SPAN

Перейти в меню **SD-WAN** → **Infrastructure** → **Контроллер SD-WAN** → **Configuration menu** → **P2P services** и нажать на кнопку **+ P2P service**.



Задать параметры сервиса P2P:

- Имя сервиса
- Выбрать сервисные интерфейсы на **CPE-1** и **CPE-4**, созданные ранее.
- **QoS : Unlimited-QoS**

New P2P service

Name

P2P-CPE-1-CPE-4-SPAN

Constraint

Threshold

Balancing mode ?

Per-flow

Description

Switch

CPE [CPE-1: 80001C57D815D7/

Service interface

Port 11, Access

Switch

CPE [CPE-4: 80001C57D815D7/

Service interface

Port 11, VLAN 2

☐ Show used interfaces

☒ Switch interfaces

☐ Use backup interface

Inbound filter

Inbound filter

QoS

Unlimited-QoS

☐ Propagate interface status

Close

Create

Нажать на кнопку **Create** для создания транспортного сервиса.

Транспортный сервис создан, теперь весь трафик, полученный на интерфейсе **eth2** устройства **CPE-1**, будет отправляться на KICS с тегом **VLAN 2** с сетевого интерфейса **eth2** устройства **CPE-4**.

3. Настройка TAP для зеркалирования трафика от транспортных сервисов

3.1. Настроить сетевые интерфейсы на CPE-2 и CPE-3

Требуется создать мост с сетевыми интерфейсами **eth2-4** на устройствах **CPE-2** и **CPE-3**.

Открыть шаблон **CPE-2** в меню **SD-WAN → CPE templates**

Выбрать вкладку **Network**.

CPE-2-template						
Information Multipathing Deactivation Encryption Scripts SD-WAN Topology Network BGP VRF OSPF Routing filters BFD Static routes Multicast VRRP						
+ Network interface						
Alias	Interface name	Protocol	IP/mask	Enable automatically		
sdwan0	eth0	DHCP client		Yes	Edit	Delete
					Disable	
sdwan1		QMI			Edit	Delete
					Disable	

Нажать на кнопку **+ Network interface** и добавить сетевые интерфейсы **lan** и **overlay** со следующими параметрами:

- **Alias** : lan
- **Zone** : lan
- **Interface name** : eth2 eth3 eth4
- Установить флажок **Bridge**
- **Protocol** : Static IPv4 address
- Установить флажок **Enable automatically**
- **IPv4 address** : 10.20.3.1
- **IPv4 Netmask** : 255.255.255.0
- **DHCP server type** : Server

New network interface

Alias

lan

Zone

lan (KICS-Training)

Interface name

eth2 eth3 eth4

☒ Bridge

Age (sec.)

300

☐ STP

NetFlow

Protocol

Static IPv4 address

Settings

☒ Enable automatically

Force IP, route, and gateway

IPv4 address and subnet mask input type

Manually

IPv4 address

10.20.21

IPv4 netmask

255.255.255.0

DHCP server

Type

Server

First IP

100

Limit

150

Lease time

12h

DHCP options

+ Add

Close

Create

- **Alias : overlay**
- **Interface name : overlay**
- **Protocol : Static IPv4 address**
- Установить флажок **Enable automatically**
- **IPv4 address : 172.16.1.3**
- **IPv4 Netmask : 255.255.255.0**

New network interface

Alias [?] overlay Zone lan (KICS-Training) Interface name [?] overlay

☐ Bridge [?]
☐ NetFlow [?]

Protocol Static IPv4 address [?]

Settings
☒ Enable automatically [?]
☐ Force IP, route, and gateway [?]

IPv4 address and subnet mask input type Manually [?]

IPv4 address [?] 172.16.1.3 IPv4 netmask [?] 255.255.255.0

IPv4 gateway [?] IPv4 broadcast [?]

DNS servers [?]
 + Add

Close Create

Повторить для шаблона **CPE-3** со следующими параметрами:

- **Alias : lan**
 - **Interface name : eth2 eth3 eth4**
 - Установить флажок **Bridge**
 - **Protocol : Static IPv4 address**
 - Установить флажок **Enable automatically**
 - **IPv4 address : 10.20.4.1**
 - **IPv4 Netmask : 255.255.255.0**
 - **DHCP Server type : Server**
-
- **Alias: overlay**
 - **Interface name : overlay**
 - **Protocol: Static IPv4 address**
 - Установить флажок **Enable automatically**
 - **IPv4 address : 172.16.1.4**
 - **IPv4 Netmask : 255.255.255.0**

3.2. Настроить BGP на CPE-2 и CPE-3

Требуется настроить карту маршрутизации для анонса сетей **lan** и BGP-соседство между устройствами **CPE-2** и **CPE-3**.

В шаблоне **CPE-2** на вкладке **Routing filters** → **Prefix lists** создать список префиксов, включающий сети **lan** устройств **CPE-2** и **CPE-3**.

В примере используются параметры:

- **Network : 10.20.0.0/26**
- **Greater or equal : 17**

New prefix list

Name ?
cpe-lans

+ Rule

Sequence	Network	Action	Greater or equal	Less or equal
10	IP/mask 10.20.0.0/16	Permit	17	

Close Create

На вкладке **Routing filters** → **Route-maps** создать карту маршрутизации, использующую список префиксов, созданный выше.

New route map

Name ?
cpe-route-maps

+ Rule

Sequence	Action	Match type	Value	Change attribute	New value
10	Permit	Prefix-List		None	

Prefix list
cpe-lans

Close Create

Настроить BGP.

На вкладке **BGP** → **General settings** задать параметры BGP:

- **AS** (автономную систему BGP)
- **Router ID** : IP-адрес сетевого интерфейса **overlay**
- **Maximum Paths** : 2
- **Graceful Restart**
- **Default IPv4 Unicast**
- **BGP Timers** :
 - **Keepalive** : 10
 - **Holdtime** : 30
- Включить редистрибуцию подключенных маршрутов (**Connected**). Применить созданную выше карту маршрутизации к подключенным маршрутам.

 **CPE-2-template**

Information · Multipathing · Deactivation · Encryption · Scripts · SD-WAN · Topology · Network **BGP**

General settings · Neighbors · Peer groups

BGP

Enabled ▾

VRF

main/254 ▾

AS

65500

Router ID

172.16.1.3

☐ Router ID from IP pool

Maximum paths

2

☐ Always compare MED

☒ Graceful restart (helper mode)

☒ Use default IPv4 unicast routes

☒ BGP timers

Keepalive

10

Holdtime

30

Route redistribution

☐ Kernel

Route map

▾

Metric

☒ Connected

Route map

cpe-route-map ▾

Metric

☐ Static

Route map

▾

Metric

На вкладке **BGP → Neighbors** создать BGP-соседство с устройством **CPE-3**.

Задать следующие параметры BGP-соседа:

- Название BGP-соседа
- IP-адрес сетевого интерфейса **overlay** устройства **CPE-3**
- Номер автономной системы устройства **CPE-3**

BGP neighbor ✕

General settings

Advanced settings

Filtering

Name

CPE-3

Shutdown BGP neighbor

☐

Neighbor IP

172.16.1.3

Remote AS

65500

Description

Password

Loopback interface

eBGP hops

☐ Custom BGP timers

☐ Enable BFD

Close

Save

Повторить настройки для шаблона **CPE-3**.

3.3. Создать сервисные интерфейсы на CPE-2 и CPE-3

Перейти в меню **SD-WAN** → **Infrastructure** → **Контроллер SD-WAN** → **Configuration menu** → **Service interfaces**.

Выбрать устройство **CPE-2**, затем нажать на кнопку **Create service interface**.

Задать параметры сервисного интерфейса:

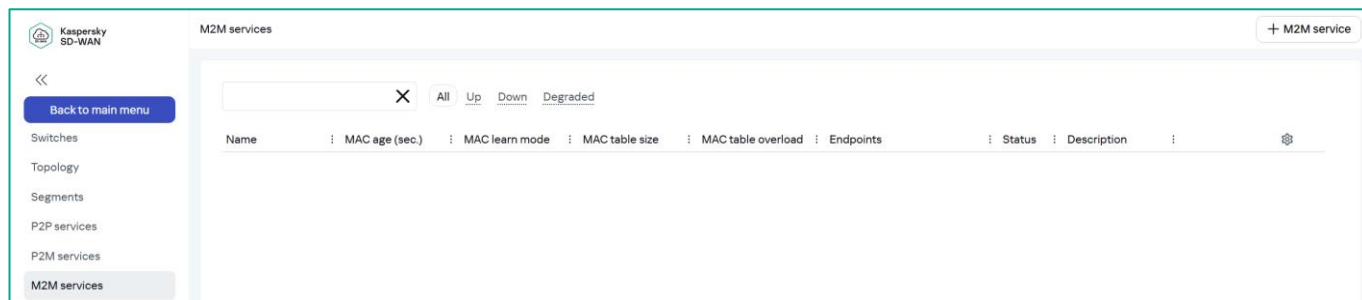
- **Port : 2 (ovs-lan)**. Этот OpenFlow-порт связан с сетевым интерфейсом **overlay** устройства CPE.
- **Type : Access** (на сервисном интерфейсе будут приниматься как тегированные, так и нетегированные кадры).

Нажать на кнопку **Create**.

Повторить для устройства **CPE-3**.

3.4. Создать транспортный сервис M2M

Перейти в меню **SD-WAN** → **Infrastructure** → **Контроллер SD-WAN** → **Configuration menu** → **M2M services** и нажать на кнопку **+M2M service**.



Задать имя сервиса и нажать на кнопку **Next**.

В секции **Service endpoints** нажать на кнопку **+ Add** и добавить сервисные интерфейсы, созданные для устройств **CPE-2** и **CPE-3**.

Задать параметры service endpoints:

- **Switch** : выбрать устройства **CPE-2** и **CPE-3** (необходимо выбрать все устройства CPE, для которых требуется организовать связность)
- **Service interface** : **Port 2 Access**
- **QoS** : **Unlimited QoS**

Нажать на кнопку **Next**.

Оставить значения по умолчанию и нажать **Create** для создания транспортного сервиса.

Транспортный сервис **M2M** создан. После установления BGP соседства **CPE-2** и **CPE-3** получат информацию о сетях **Ian** друг-друга, что позволит обеспечить IP-связность между площадками.

3.5. Создать TAP для зеркалирования трафика на CPE-4

Для отправки копии трафика на KICS с M2M-сервиса требуется настроить TAP-сервис, указав **CPE-4** как точку назначения зеркалирования.

Перейти в меню **SD-WAN → Infrastructure → Контроллер SD-WAN → Configuration menu → Service interfaces**.

Service interfaces

Switch: CPE [CPE-1: 80001C57D815D7] Port: All Create service interface

Port	Type	Description	VLAN	Inner VLAN	Filter	Name	
2	Access					SI://CPE [CPE-1: 80001C57D815D727]/p:2	Management

Выбрать **CPE-4**, затем нажать на кнопку **Create service interface**.

Задать параметры сервисного интерфейса:

- **Port : eth2**
- **Type : VLAN**
- **VLAN ID : 3**

Нажать на кнопку **Create**.

Note: На OpenFlow-порту невозможно одновременно настроить сервисный интерфейс с классификацией Access и VLAN/QinQ.

New service interface

Port: 12 (eth2)

Type: VLAN

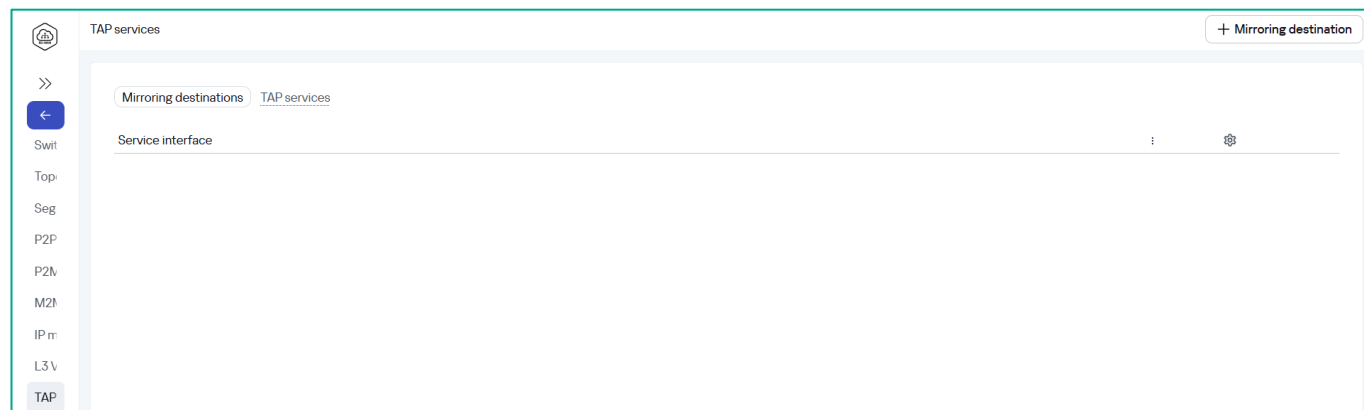
VLAN ID: 3

Description:

Close Create

Перейти в меню **TAP services** → **Mirroring destinations**.

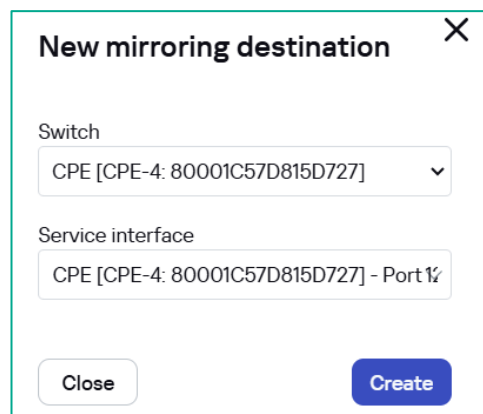
Нажать на кнопку **+ Mirroring destination** для создания новой точки назначения зеркалирования.



Задать параметры точки назначения зеркалирования:

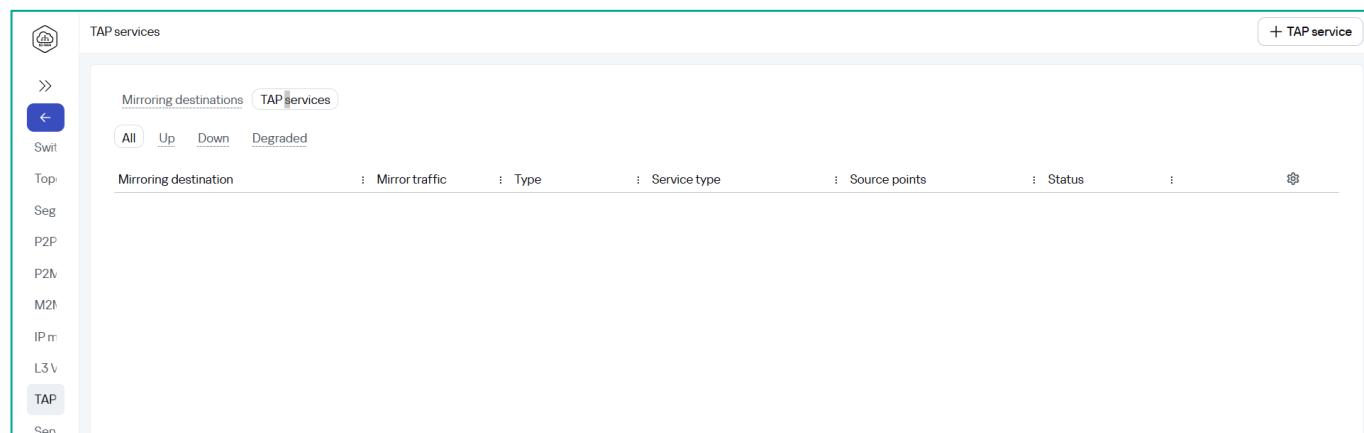
- **Switch** : **CPE-4**
- **Service interface** : сервисный интерфейс **CPE-4 eth2 VLAN 3**

Нажать на кнопку **Create** для создания точки назначения зеркалирования.



Выбрать вкладку **TAP services**.

Нажать на кнопку **+ TAP service** для создания нового TAP-сервиса.



Задать параметры сервиса **TAP**:

- Установить флажок **Mirror traffic**
- **Mirroring destination** : **CPE-4 VLAN-3**
- **Source point type** : **Transport service**
- **Type** : **M2M**
- **Transport service** : выбрать транспортный сервис, созданный в п. 3.4
- **Source points** : выбрать все сервисные интерфейсы, добавленные в M2M-сервис (**CPE-2** и **CPE-3**)

Нажать на кнопку **Next**.

New TAP service

☒ Mirror traffic

Balancing mode [?]
 Per-flow

Mirroring destination
 CPE [CPE-4: 80001C57D815D727]-12

Source point type
 Transport service

Type
 M2M

Transport service
 L2 M2M
 L2 M2M Delete

Source points
 CPE [CPE-2: 80001C57D815D755]-2 Delete

Close

Next

Нажать на кнопку **Create** для создания TAP-сервиса.

New TAP service

Qualification rules:
 CPE [CPE-2: 80001C57D815D755]-2

Close

Back

Create

TAP-сервис создан, теперь копия трафика с M2M-сервиса между устройствами **CPE-2** и **CPE-3** будет отправляться с сетевого интерфейса **eth2** устройства **CPE-4** с тегом VLAN 3.

4. Приложение А. Настройка передачи тегированного трафика через SD-WAN

В этой секции описан пример для передачи тегированного трафика от коммутаторов с удаленных площадок через транспортный сервис P2P.

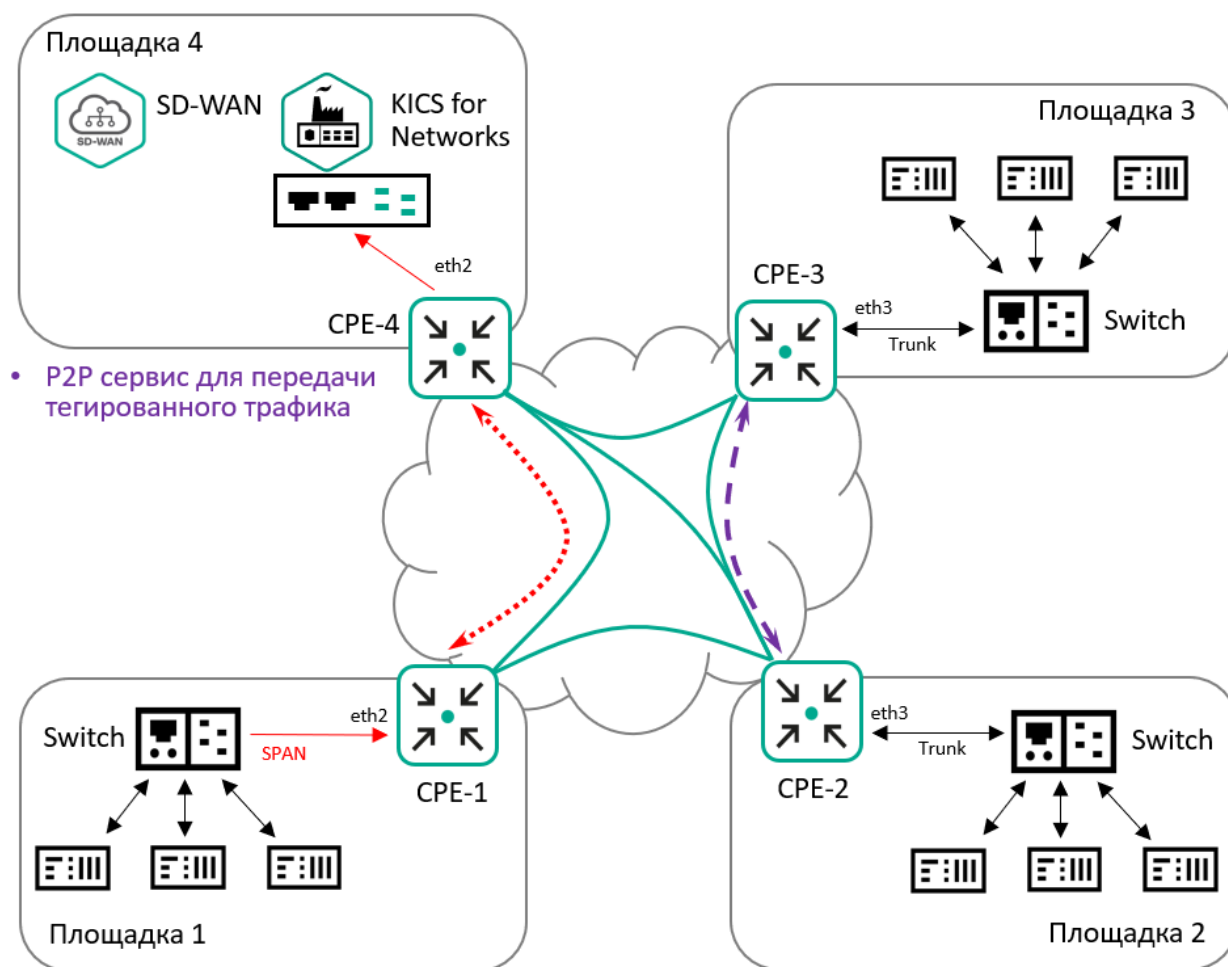


Рисунок 1 – Схема передачи тегированного трафика через сервис P2P

Устройства CPE-2 и CPE-3 получают тегированный трафик от внешних коммутаторов на сетевые интерфейсы eth3. На устройствах CPE-2 и CPE-3 сетевые интерфейсы eth3 переведены в режим L2 для прямой работы в Open vSwitch, что позволяет настроить сервисные интерфейсы непосредственно на физических портах. На устройствах CPE-2 и CPE-3 созданы сервисные интерфейсы с классификацией Access на сетевых интерфейсах eth3, которые принимают весь трафик от внешних коммутаторов. Для отправки трафика между устройствами CPE-2 и CPE-3 создан транспортный сервис P2P.

4.1. Перевести интерфейсы eth3 в режим L2 на CPE-2 и CPE-3.

Требуется перевести сетевые интерфейсы **eth3** на **CPE-2** и **CPE-3** в режим **L2**.

Открыть шаблон **CPE-2** в меню **SD-WAN → CPE templates**

Выбрать вкладку **Network**.

CPE-2-template

Information Multipathing Deactivation Encryption Scripts SD-WAN Topology **Network** BGP VRF OSPF Routing filters BFD Static routes

+ Network interface

Alias	Interface name	Protocol	IP/mask	Enable automatically	
overlay	overlay	Static IPv4 address	IP: 172.16.1.2 Mask: 255.255.255.0	Yes	Edit Delete Disable
sdwan0	eth0	DHCP client		Yes	Edit Delete Disable
sdwan1		QMI			Edit Delete Disable

Нажать на кнопку **+ Network interface** и добавить сетевой интерфейс **eth2** со следующими параметрами:

- **Alias** : eth3
- **Interface name** : eth3
- **Protocol** : None
- Установить флажок **L2 mode** для перевода интерфейса в режим **L2**
- Установить флажок **Enable automatically**

New network interface ✕

Alias ? eth3 Interface name ? eth3

Protocol
None

☒ L2 mode ?

OpenFlow port ?
11

⚠ To enable L2 mode, you must create a service interface mapped to the specified OpenFlow port in the controller configuration menu

Settings
☒ Enable automatically ?

Override MAC ? Override MTU ?

Close Create

Повторить для шаблона **CPE-3**.

4.2. Создать сервисные интерфейсы на CPE-2 и CPE-3

Перейти в меню **SD-WAN** → **Infrastructure** → **Контроллер SD-WAN** → **Configuration menu** → **Service interfaces**.

Выбрать **CPE-2**, затем нажать на кнопку **Create service interface**.

Задать параметры сервисного интерфейса:

- **Port** : eth2
- **Type** : **Access** (на сервисном интерфейсе будут приниматься как тегированные, так и нетегированные кадры)

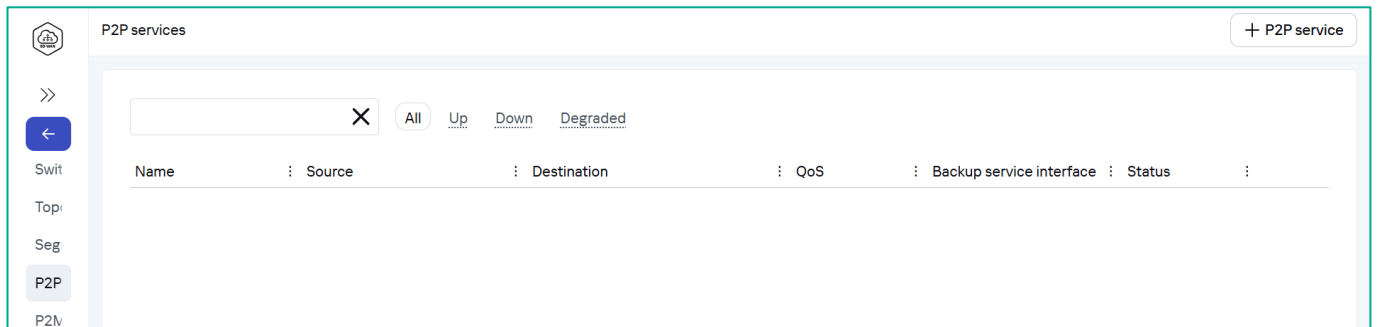
Нажать на кнопку **Create**.

Note: На OpenFlow-порту невозможно одновременно настроить сервисный интерфейс с классификацией Access и VLAN / Q-in-Q.

Повторить для **CPE-3**.

4.3. Создать транспортный сервис P2P

Перейти в меню **SD-WAN → Infrastructure → Контроллер SD-WAN → Configuration menu → P2P services** и нажать на кнопку **+ P2P service**.



Задать параметры сервиса P2P:

- Имя сервиса
- Выбрать сервисные интерфейсы **CPE-2** и **CPE-3**, созданные ранее.
- **QoS : Unlimited-QoS**

New P2P service

Name

P2P-Trunk-CPE-2-CPE-3

Constraint

Threshold

Balancing mode ?

Per-flow

Description

Switch

CPE [CPE-2: 80001C57D815D7/

Service interface

Port 12, Access

Switch

CPE [CPE-3: 80001C57D815D7/

Service interface

Port 12, Access

☐ Show used interfaces
 ☒ Switch interfaces
 ☐ Use backup interface

Inbound filter

Inbound filter

QoS

Unlimited-QoS

☐ Propagate interface status

Close

Create

Нажать на кнопку **Create** для создания транспортного сервиса.

Транспортный сервис создан, теперь тегированный трафик, полученный интерфейсами **eth3 CPE-2** и **CPE-3**, будет отправляться через транспортный сервис P2P.