



Networking
For everyone

MPLS L2 VPN

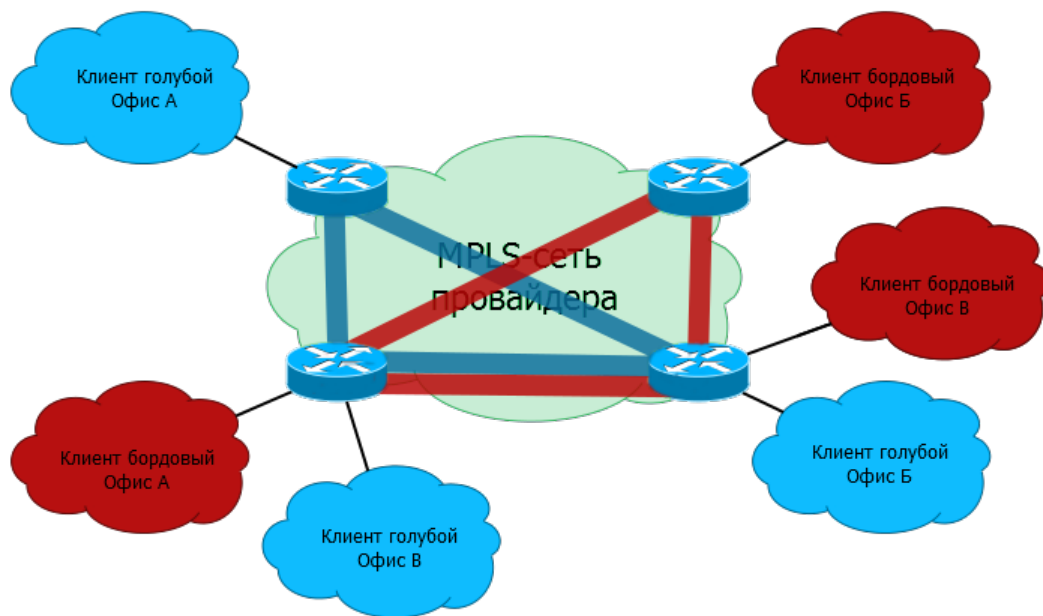
Распространённые технологии

- VLAN/QinQ
- L2TPv3/PPTP
- EVPN
- MPLS L2VPN

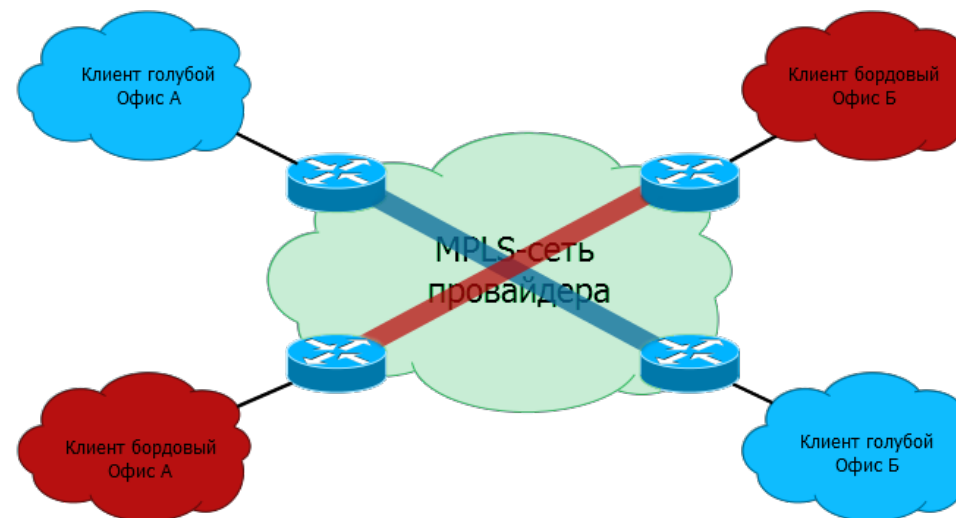
Классификация L2VPN

- P2P
 - Virtual Private Wire Service (VPWS)
- P2MP
 - Virtual Private LAN Service (VPLS)

VPLS. Точка-многоточка



VPWS. Точка-точка



Терминология

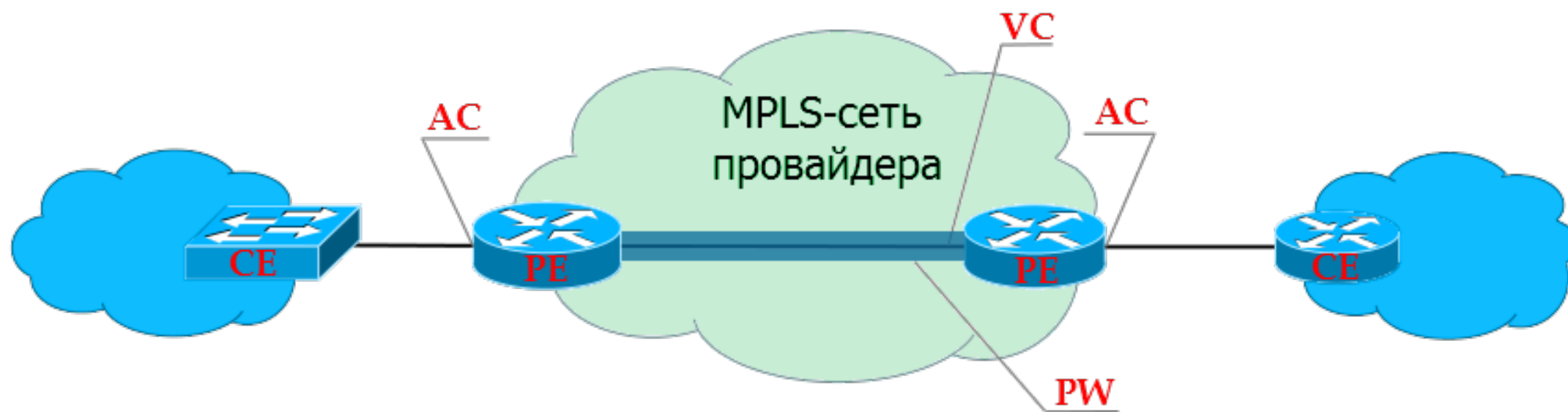
- **PE** — Provider Edge — граничные маршрутизаторы MPLS-сети провайдера, к которым подключаются клиентские устройства (CE).

CE — Customer Edge — оборудование клиента, непосредственно подключающееся к маршрутизаторам провайдера (PE).

AC — Attached Circuit — интерфейс на PE для подключения клиента.

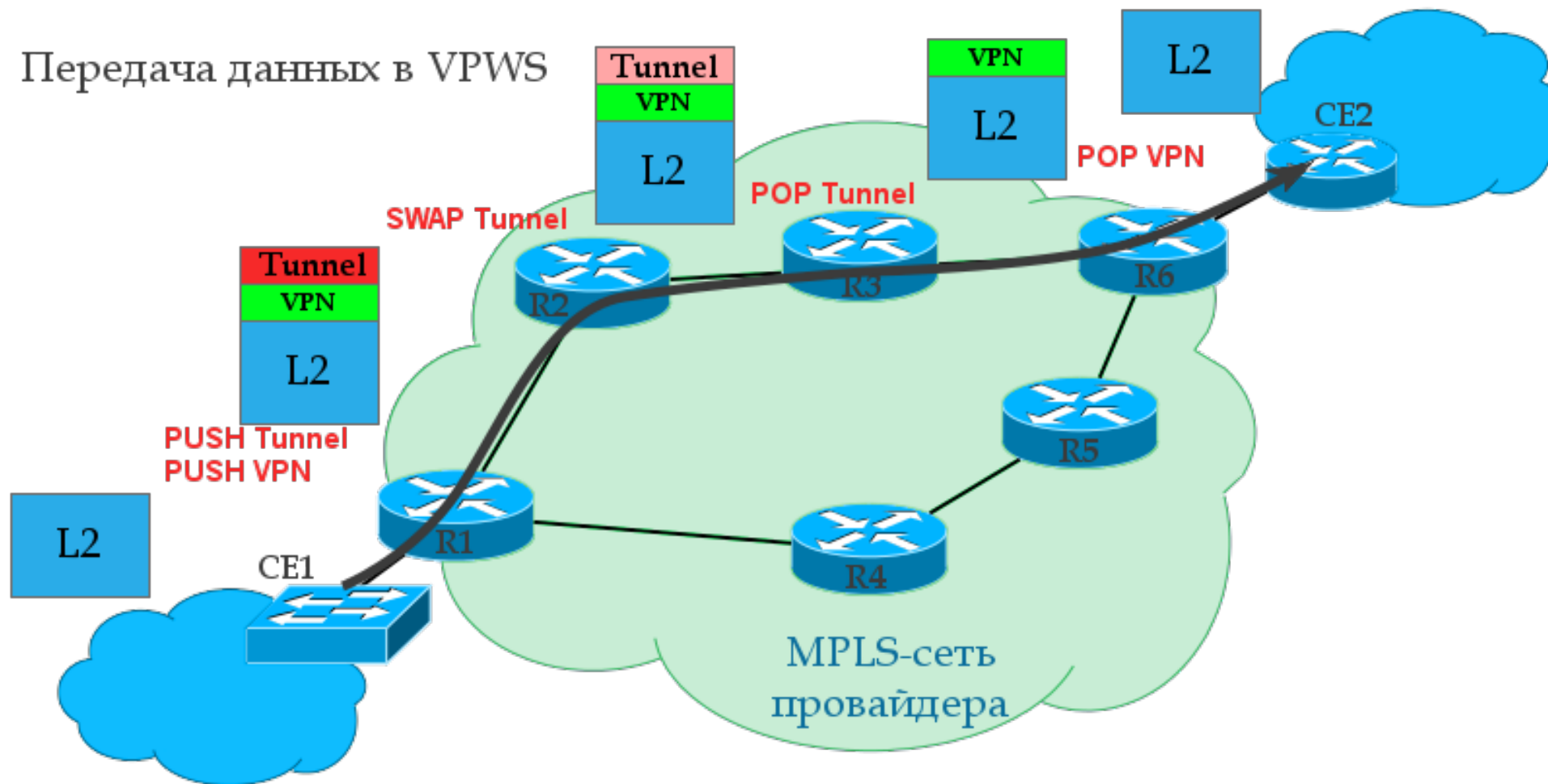
VC — Virtual Circuit — виртуальное однонаправленное соединение через общую сеть, имитирующее оригинальную среду для клиента. Соединяет между собой AC-интерфейсы разных PE. Вместе они составляют цельный канал: AC→VC→AC.

PW — PseudoWire — виртуальный двунаправленный канал передачи данных между двумя PE — состоит из пары однонаправленных VC. В этом и есть отличие PW от VC.



VPWS Data Plane

Передача данных в VPWS





Networking
For everyone

VPWS

VPWS

- Транспортная метка назначается посредством LDP или RSVP TE
- Сервисная метка назначается с помощью *targeted LDP*
- Основные реализации
 - Layer 2 over IP
 - L2TPv3
 - Layer 2 over MPLS
 - Any Transport over MPLS (AToM)

AToM

- Абсолютно не важен тип полезной нагрузки
 - это может быть FR, ATM, PPP и т.д.
- Два режима работы
 - same-to-same
 - Ethernet в Ethernet, PPP в PPP и т.д.
 - Interworking
 - Ethernet в PPP, ATM в FR и т.д.

```
pseudowire-class ethernet-port  
  encapsulation mpls  
!  
int gigabitethernet1/0  
  xconnect 10.0.0.1 123 pw-class ethernet-port
```



Interworking

- PE1

```
pseudowire-class atom-eth-iw
 encapsulation mpls
 interworking ethernet
!
interface Loopback0
 ip address 10.8.8.8 255.255.255.255
!
interface FastEthernet1/0.1
 encapsulation dot1q 100
 xconnect 10.9.9.9 123 pw-class atom-eth-iw
```

- PE2

```
pseudowire-class atom
 encapsulation mpls
!
interface Loopback0
 ip address 10.9.9.9 255.255.255.255
!
interface FastEthernet0/0
 no ip address
!
interface FastEthernet1/0
 xconnect 10.9.9.9 123 pw-class atom
```



Отказоустойчивость

```
interface Ethernet0/0  
  xconnect 10.55.55.2 1000 pw-class mpls-ip  
  backup peer 10.55.55.3 1001 pw-class mpls-ip
```

IOS XR

- Настройка

```
RP/0/0/CPU0:PE1(config)#int gig0/0/0/4 l2transport
RP/0/0/CPU0:PE1(config-if-l2)#commit
```

```
RP/0/0/CPU0:PE1(config)#l2vpn
RP/0/0/CPU0:PE1(config-l2vpn)#xconnect group TEST
RP/0/0/CPU0:PE1(config-l2vpn-xc)#p2p wire1
RP/0/0/CPU0:PE1(config-l2vpn-xc-p2p)#interface GigabitEthernet0/0/0/4
RP/0/0/CPU0:PE1(config-l2vpn-xc-p2p)#neighbor 3.3.3.3 pw-id 101
RP/0/0/CPU0:PE1(config-l2vpn-xc-p2p-pw)#commit
```

- Проверка

```
RP/0/0/CPU0:PE1#show l2vpn xconnect detail
```



Networking
For everyone

VPLS

VPLS. Терминология

- VPLS-домен — изолированная виртуальная L2-сеть, то есть, грубо говоря, один отдельный L2VPN.
 - Два разных клиента — два разных VPLS-домена.
- **VSI** — Virtual Switching Instance. Виртуальный коммутатор в пределах одного узла.
 - Для каждого клиента (или сервиса) он свой.
 - Аналог VRF в L3VPN
- **VE** — VPLS Edge — узел PE, участник VPLS-домена.

VPLS Data Plane

- В целом, VPLS домен очень похож на структуру VLAN коммутатора
 - Присутствует MAC learning и Split Horizon
- VSI/VFI является виртуальным overlay интерфейсом вообразаемого коммутатора
- В вопросе изучения MAC-адресов в VPLS есть нюанс
 - PE важно определить соседа или, точнее PW как виртуальный интерфейс. Дело в том, что клиентский кадр нужно отправить не просто в какой-то физический порт, а именно в правильный PW, иными словами, правильному соседу
 - Для этой цели каждому соседу выдаётся личная метка

VPLS Control Plane

- для VPLS требуется полносвязная топология PE для каждого VSI. Причём не все PE MPLS-сети провайдера будут соседями, а только те, где есть этот же VSI
- один из главных вопросов в VPLS — обнаружение всех PE, куда подключены клиенты данного VSI
- Два основных подхода к решению вопроса
 - Ручная настройка (Martini)
 - RFC 4762 Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
 - Автоматическое обнаружение (Kompella)
 - RFC 4761 Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling

VPLS Martini

- Распределение сервисных меток с помощью LDP
- Идея такая же, как в VPWS
 - Полносвязная tLDP топология
- Если состояние AC-порта VPLS-домена переходит в Down, то PE сообщает об этом всем своим соседям, с помощью LDP MAC Withdraw

VPLS Kompella

- Альтернативное название - VPLS Auto-Discovery
- В секции BGP для VPLS есть своя Address Family: L2VPN AFI (25) и VPLS SAFI (65)
- Обнаружение соседей аналогично VPNv4 (на основе RT)
 - Если RT полученного анонса совпадает с настроенным в VSI, значит этот VSI хочет знать информацию из анонса

VPLS NLRI

- Формально, префикс — это RD+порядковый номер узла в VPLS-домене+**блок меток**
- Блок меток
 - VE ID
 - VE Block Offset
 - VE Block Size
 - Label Base

Блок меток

- VE ID—идентификатор PE-маршрутизатора в домене VPLS
- **LB** — Label Base — первая метка, которая может быть использована
- **VBS** — VE Block Size — это длина блока меток
- Метки выделяются по порядку
- https://kb.juniper.net/library/CUSTOMERSERVICE/technotes/Understanding_VPLS_Label_Blocks_Operation.pdf

Как распределяются метки между соседями

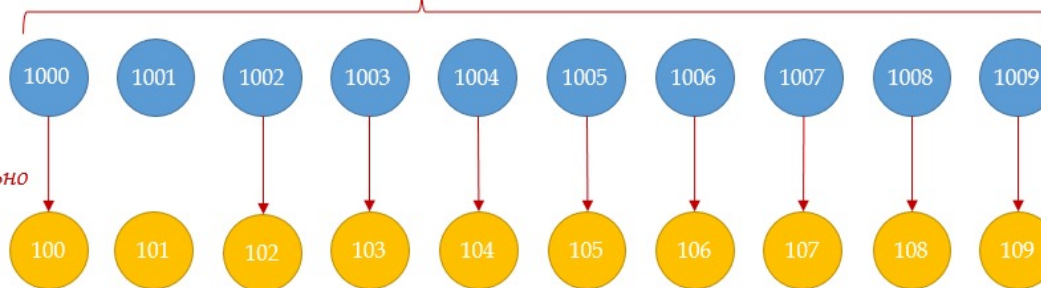
PE1:

VE ID: 101, Label Block Base: 1000, VBS: 10, VE ID: 100-109

Диапазон меток

*Очень просто:
всегда последовательно*

Соседи



MPLS L2 VPN



Networking
For everyone

Возможен и третий вариант

- BGP Autodiscovery + LDP Signalling
- В этом случае BGP отвечает только за поиск соседей, а за назначение сервисных меток отвечает tLDP



Networking
For everyone

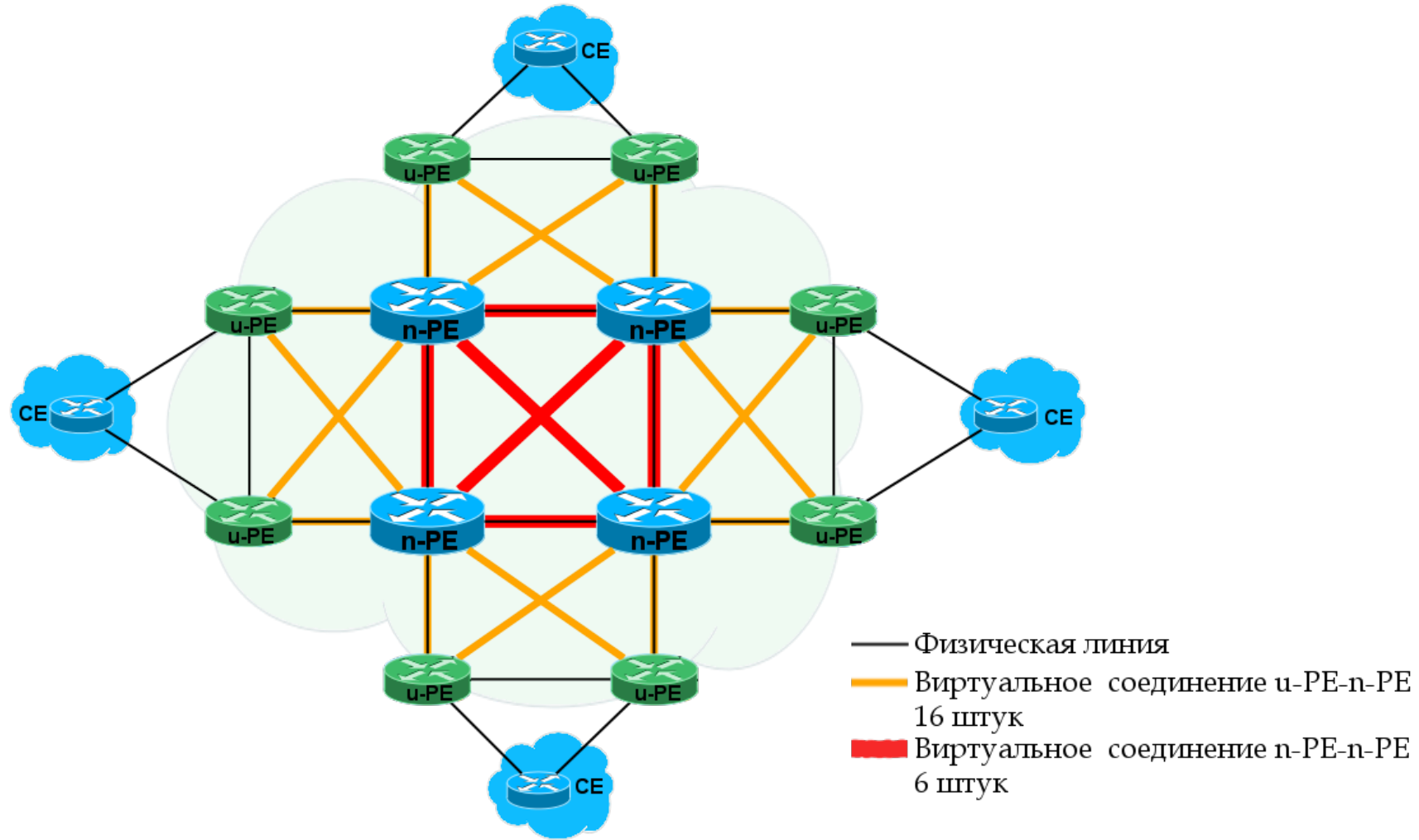
Иерархический
VPLS

Иерархический VPLS

- Большое количество PE ведёт к большому числу tLDP сессий и огромному количеству PW
- Приходится много раз делать репликацию для широковещательных пакетов
- Решение – иерархический VPLS (H-VPLS)

Архитектура H-VPLS

- **PE-rs** — PE — routing and switching. Это ядро сети VPLS. Это большие производительные железки, которые функционируют как обычные PE (n-PE)
- **MTU-s** — Multi-Tenant Unit — switching. Это могут быть более слабые устройства, которые подключаются к PE-rs с одной стороны. А с другой к ним подключаются CE (u-PE)



- Механизмы подключения MTU-s к PE-rs: MPLS PW или QinQ
- PE-rs между собой взаимодействуют как обычные PE, образуя полносвязную топологию
- При взаимодействии PE-rs и MTU-s, PE-rs воспринимает PW от MTU-s как AC-интерфейс

Преимущества VPLS

- Улучшение масштабируемости сети в плане Control Plane
- Оптимизация Data Plane за счёт уменьшения числа копий широковещательных кадров
- Возможность делить VPLS-домен на сегменты и ставить на доступ более дешёвое оборудование

Всё ли так радужно?

- То, что в обычном VPLS было P, в H-VPLS стало PE
 - Надо изучать MAC-адреса. Причём от всех MTU-s, которые к нему подключены. А вместе с тем заниматься рассылкой и репликацией клиентских кадров.
- Введя иерархию на Control Plane мы форсировали создание иерархии и на Data Plane.
- Справившись с одной проблемой масштабируемости, H-VPLS создал новую.
 - Счёт MAC-адресов в этом случае может идти на тысячи и сотни тысяч



Networking
For everyone