



OTUS

ОНЛАЙН-ОБРАЗОВАНИЕ

# Онлайн-образование



# Меня хорошо видно && слышно?

Ставьте +, если все хорошо  
Напишите в чат, если есть проблемы

# Технологии построения сетевых фабрик



Кулиничев Алексей

Администратор Сетей

[Santhous42@yandex.ru](mailto:Santhous42@yandex.ru)

# Правила вебинара



Активно участвуем



Задаем вопрос в чат или голосом



Off-topic обсуждаем в Slack #канал группы или #general



Вопросы вижу в чате, могу ответить не сразу

# Маршрут вебинара

Основы разделения сети



Underlay



Overlay



SD-Access

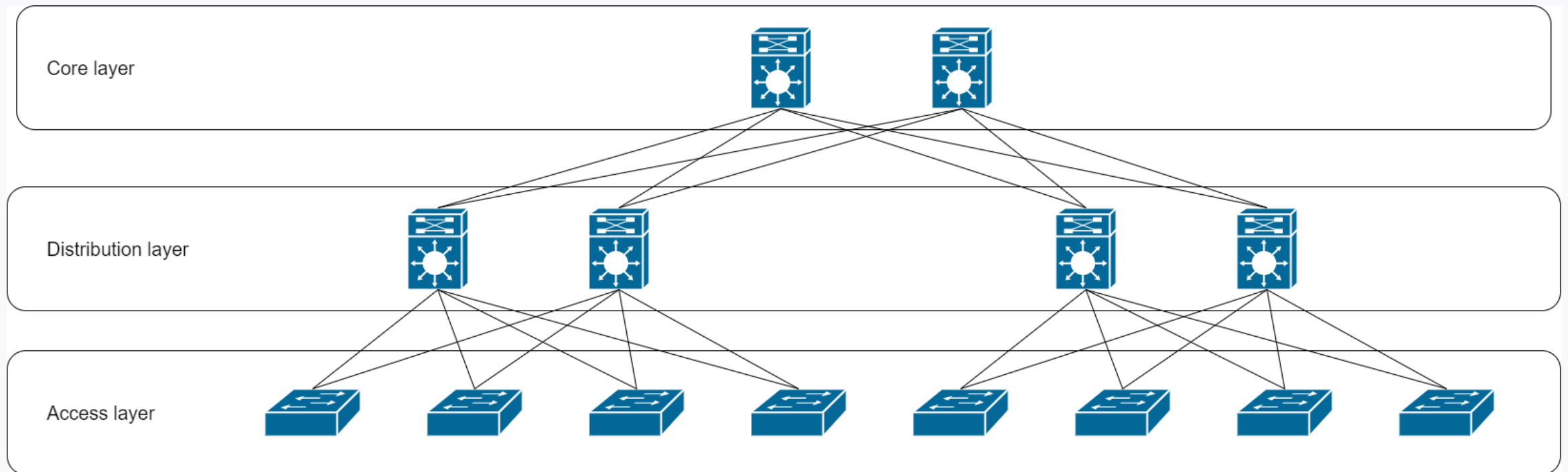


# 1

ОСНОВЫ



# ОСНОВЫ



# ОСНОВЫ

- Не хватает количества VLAN – 4096
- Огромное количество mac адресов – на каждом физическом сервере может находиться до нескольких сотен виртуалок
- Мобильность – простота переноса сервера (пользователя)
- Независимость от расположения – сервер может быть подключен в любую часть сети с сохранением доступности
- Full-mesh – любой сервис может быть связан с любым другим через L2
- Необходимость использовать STP

Необходимы новые протоколы для решения всех задач



Новые протоколы – новые технологии – новое оборудование

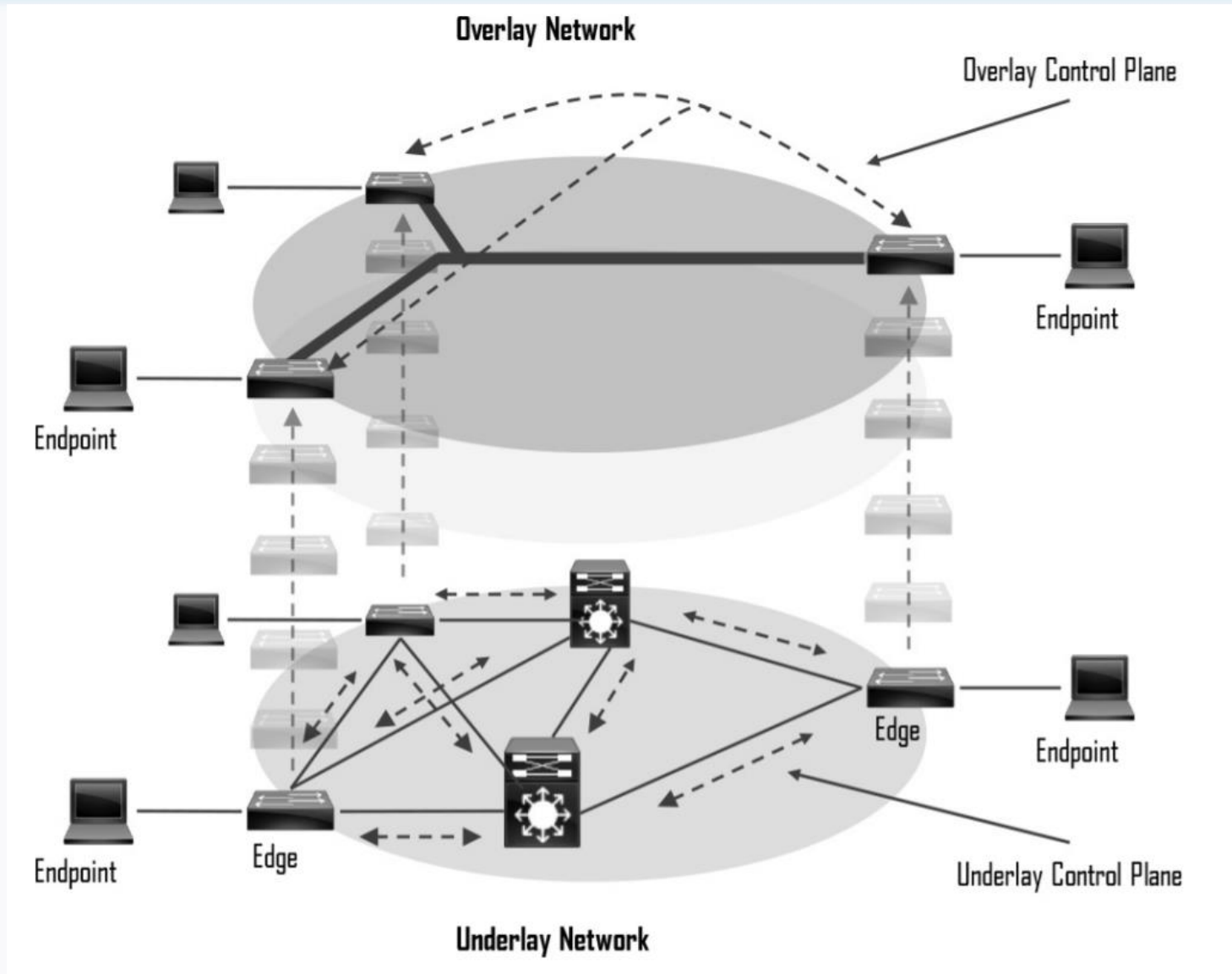


Трудоемкий и экономически не эффективный метод решения

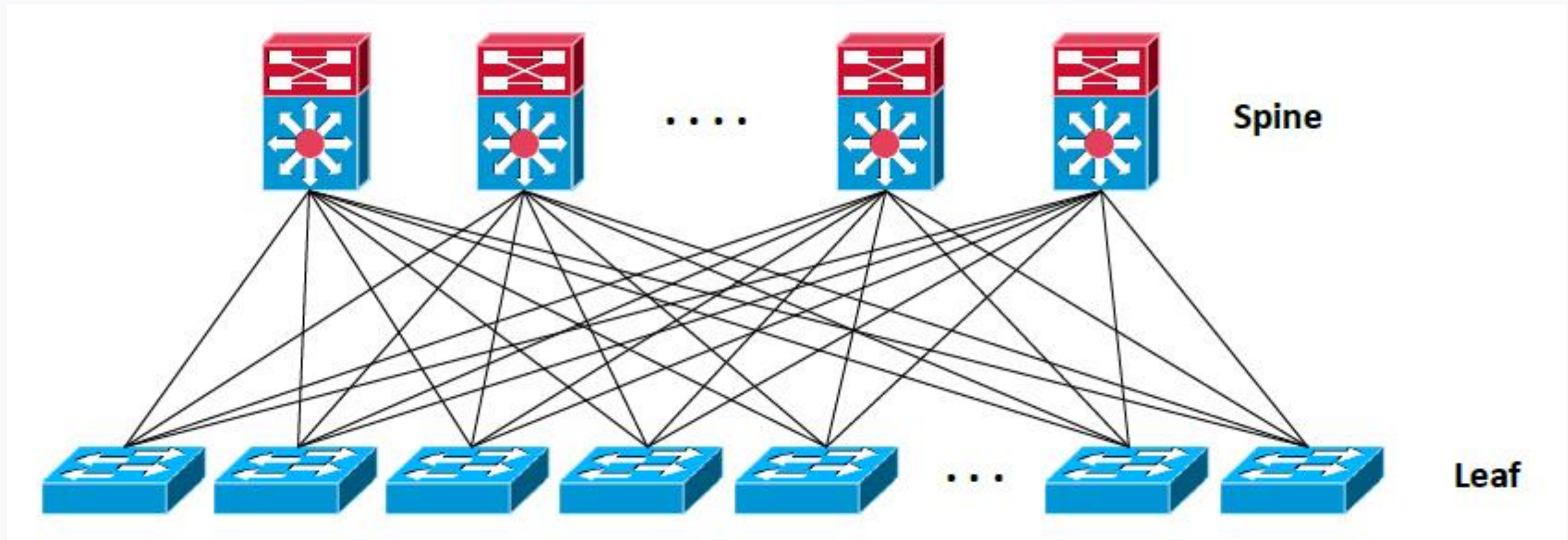


Overlay сети

# ОСНОВЫ



## Архитектура сети – CLOS



Преимущества разделения сети на два уровня:

Изменение или ошибки на одном уровне не влияют на другой уровень сети

# ОСНОВЫ

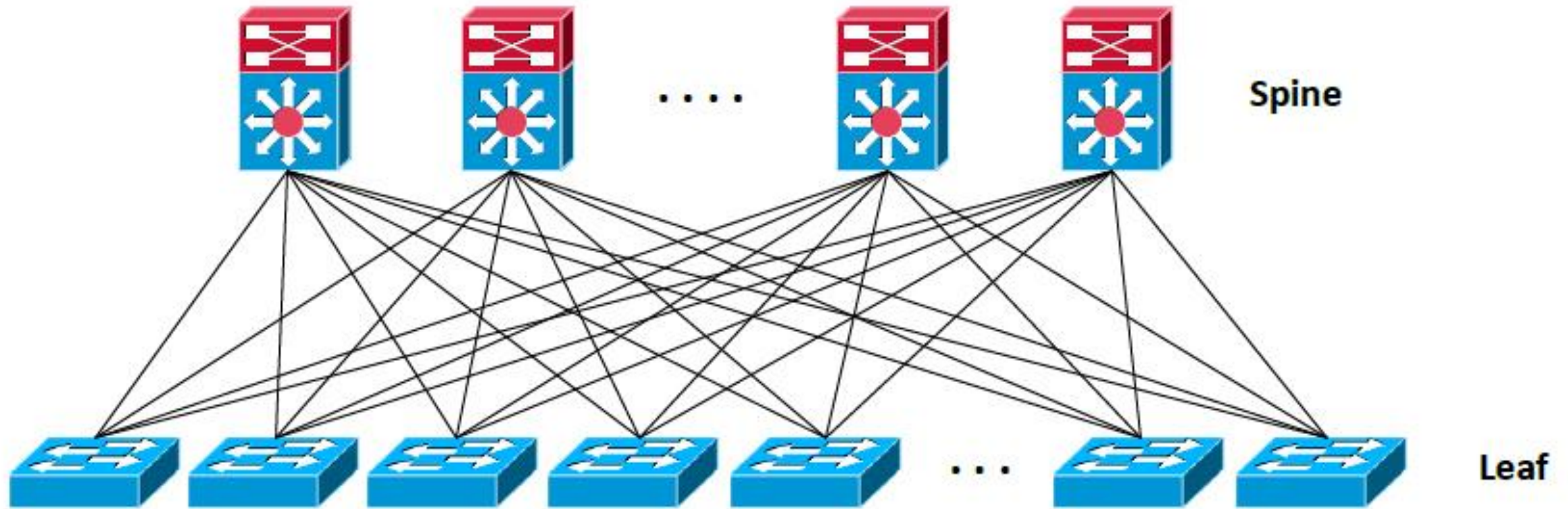
|            | Тип Overlay                  | Где используется                         | Транспорт   |
|------------|------------------------------|--|-------------|
| FabricPath | Network-based                | Внутри ЦОД                               | FabricPath* |
| TRILL      | Network-based                | Внутри ЦОД                               | TRILL*      |
| VXLAN      | Host-based или Network-based | Как внутри ЦОД, так и между ЦОД          | UDP         |
| OTV        | Network-based                | Между ЦОД                                | UDP         |
| LISP       | Network-based                | Передачи трафика к ВМ, которые мигрируют | UDP         |



# 2 Underlay



# Underlay



# Underlay

Underlay – основа сети: физическое оборудование, каналы, кабели и прочее аппаратная часть сети.

Основная задача – знать как добраться от одного хоста до другого

Внутри сети underlay только L3 связанность

# Underlay

Между устройствами в Underlay для обеспечения IP связанности используется:

- BGP
- OSPF
- ISIS
- EIGRP
- L2+STP
- Т.д.



# 3 Overlay



# Overlay

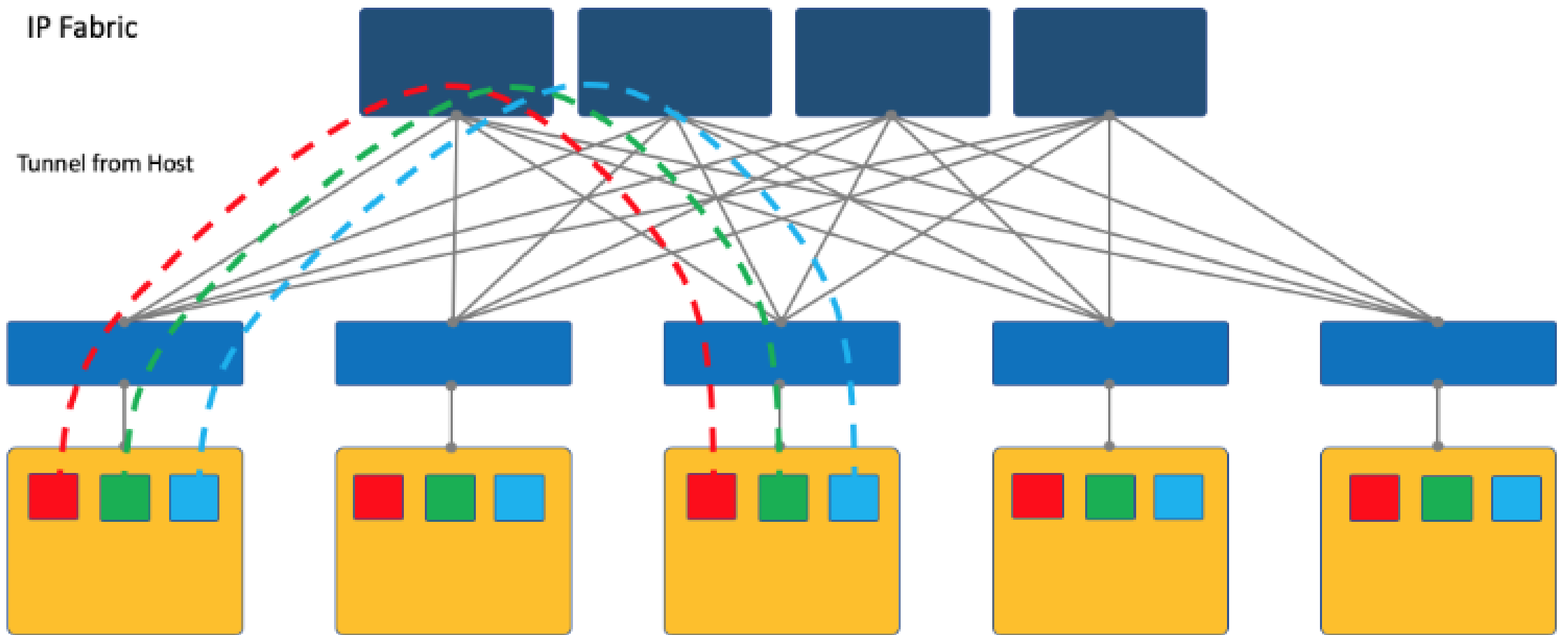
## Network Based:

- Железо должно поддерживать технологию
- Повышенные требования к MAC-таблице для ToR (Top-of-Rack) коммутаторов

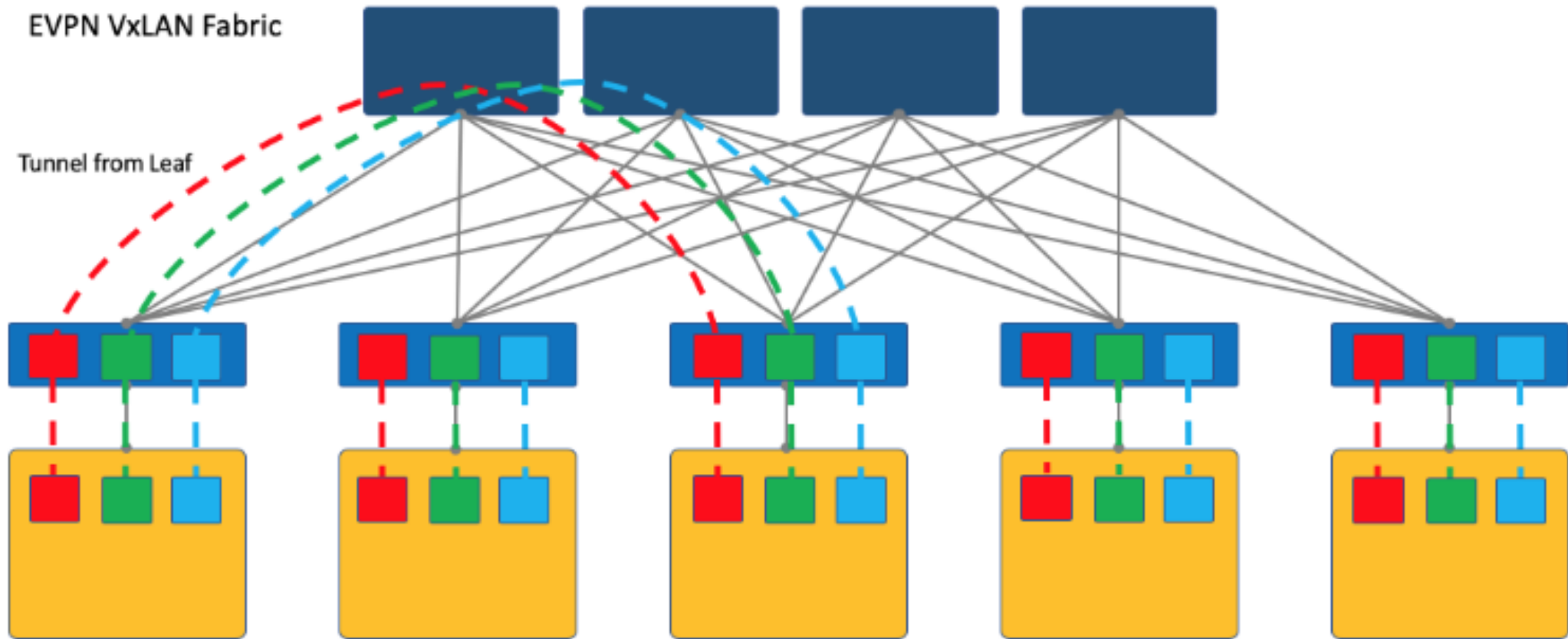
## Host Based:

- Нет информации о топологии сети
- Возможные проблемы с производительностью, так как процесс инкапсуляции/декапсуляции выполняет сам хост

# Overlay



# Overlay





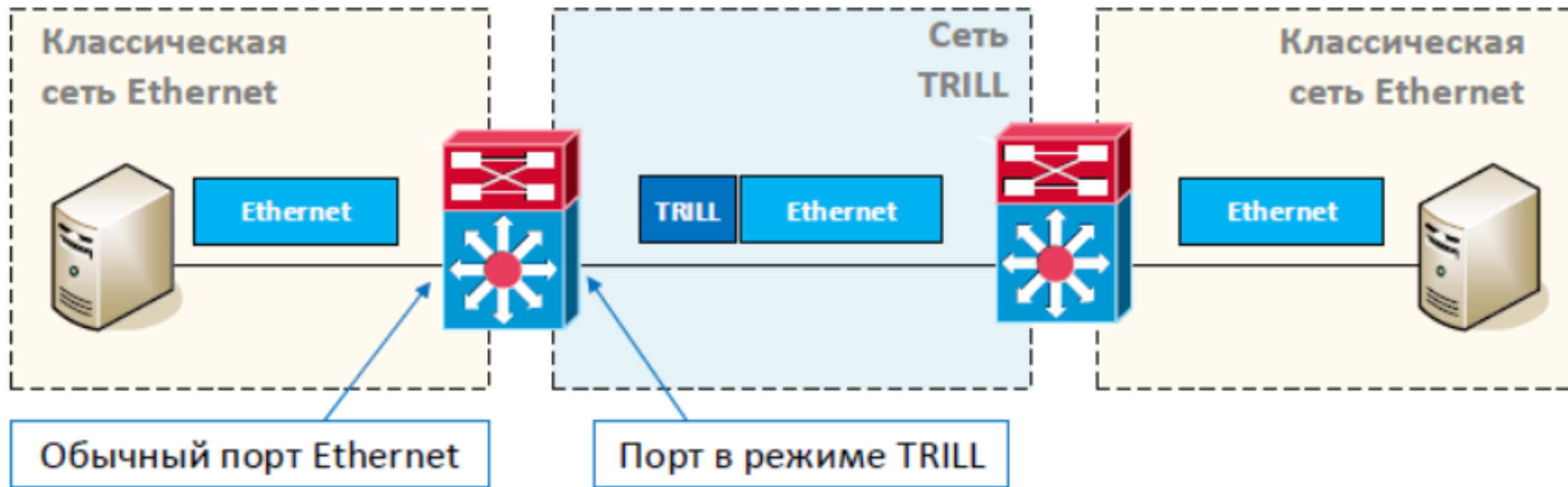
# 3.1

TRILL/FabricPath

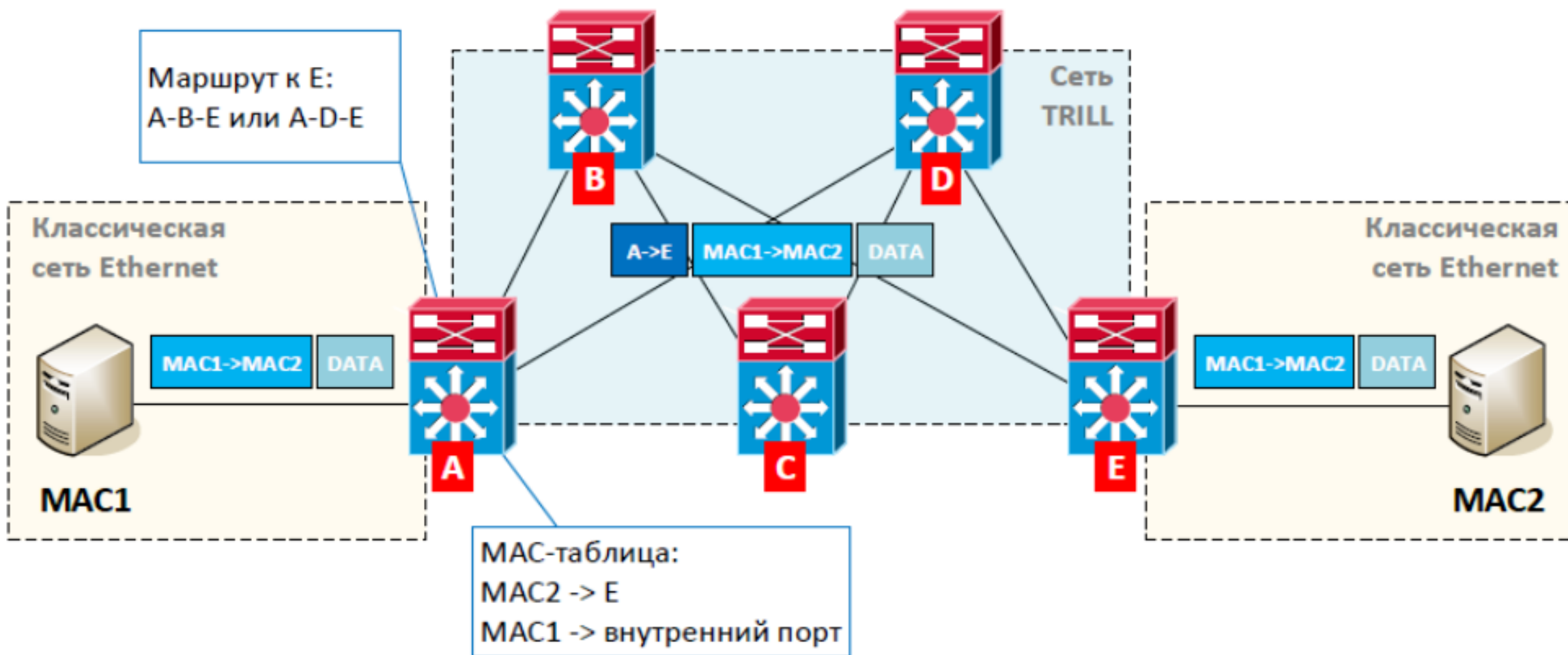


# TRILL/FabricPath

Распределённые сегменты являются одним общим L2-доменом



# TRILL/FabricPath



# TRILL/FabricPath

## Плюсы:

- Маршрутизация на основе меток TRILL на уровне L2. То есть избавляемся от STP
- Равномерная утилизация каналов с одинаковыми маршрутами
- Поддерживает передачу любых сообщений на уровнях выше (ISIS)

## Недостатки:

- У разных вендоров свои реализации TRILL (FabricPath – Cisco)
- Используется в рамках одного ЦОД
- Дорогостоящее оборудование



3 OTV 2



OTV – Overlay Transport Virtualization, разработан компанией Cisco для растягивания L2 между ЦОД

В рамках самого ЦОД планировалось использовать FabricPath

Используется протокол ISIS. По сути реализуется маршрутизации по MAC адреса.

Поддерживается два режима работы:

1. Multicast
2. Unicast

## Multicast:

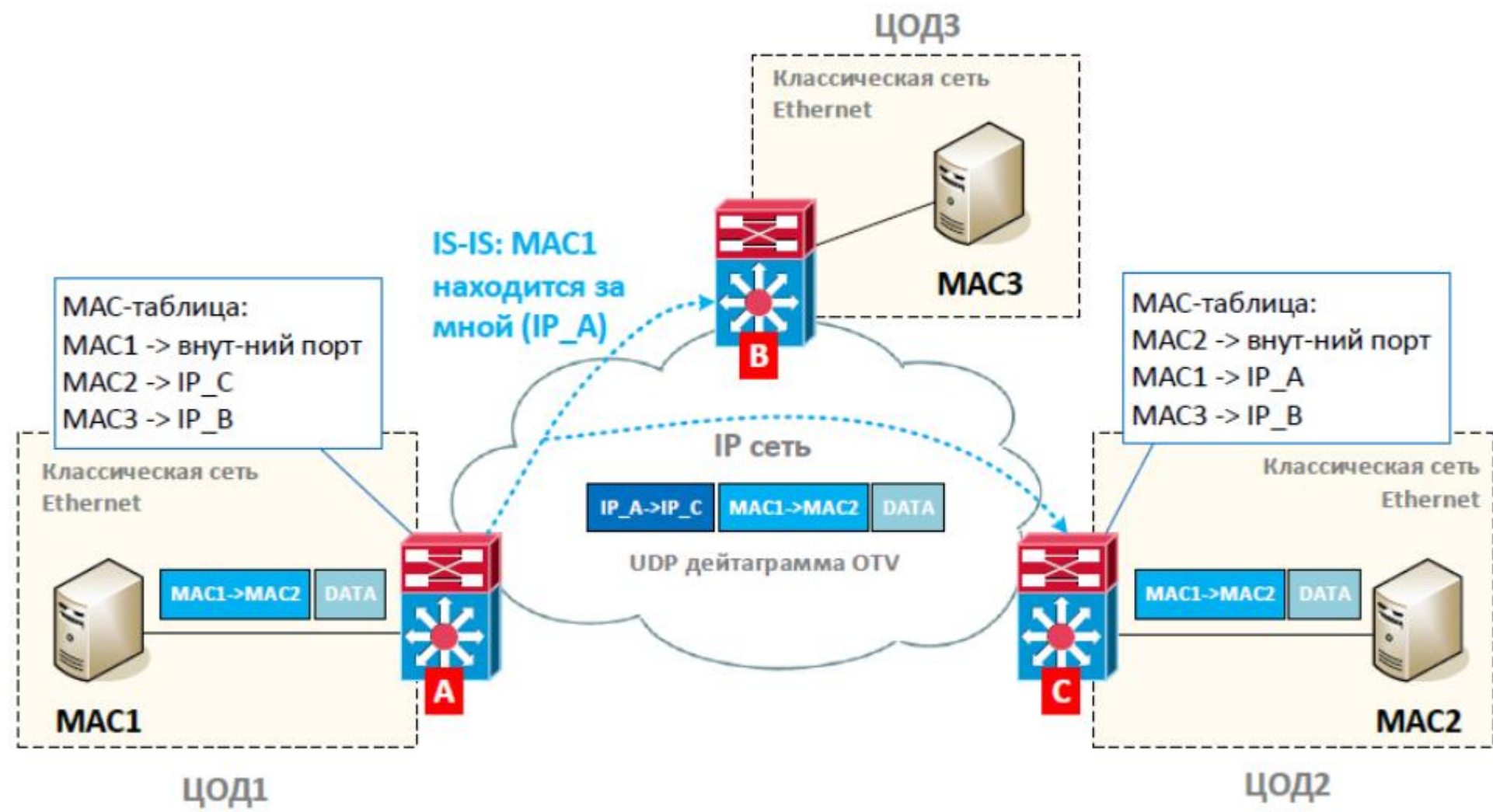
Сеть должна поддерживать маршрутизацию multicast (трудно реализуемо между ЦОД)

## Unicast:

Выделяется специальный сервер(на каждом устройстве указывается в ручную) – Adjacency Server, который принимает все анонсы, а потом дублирует на остальные узлы сети OTV.

Получив информацию о другом соседе мы можем установить с ним соединение через unicast напрямую

# OTV





# 3.3

LISP

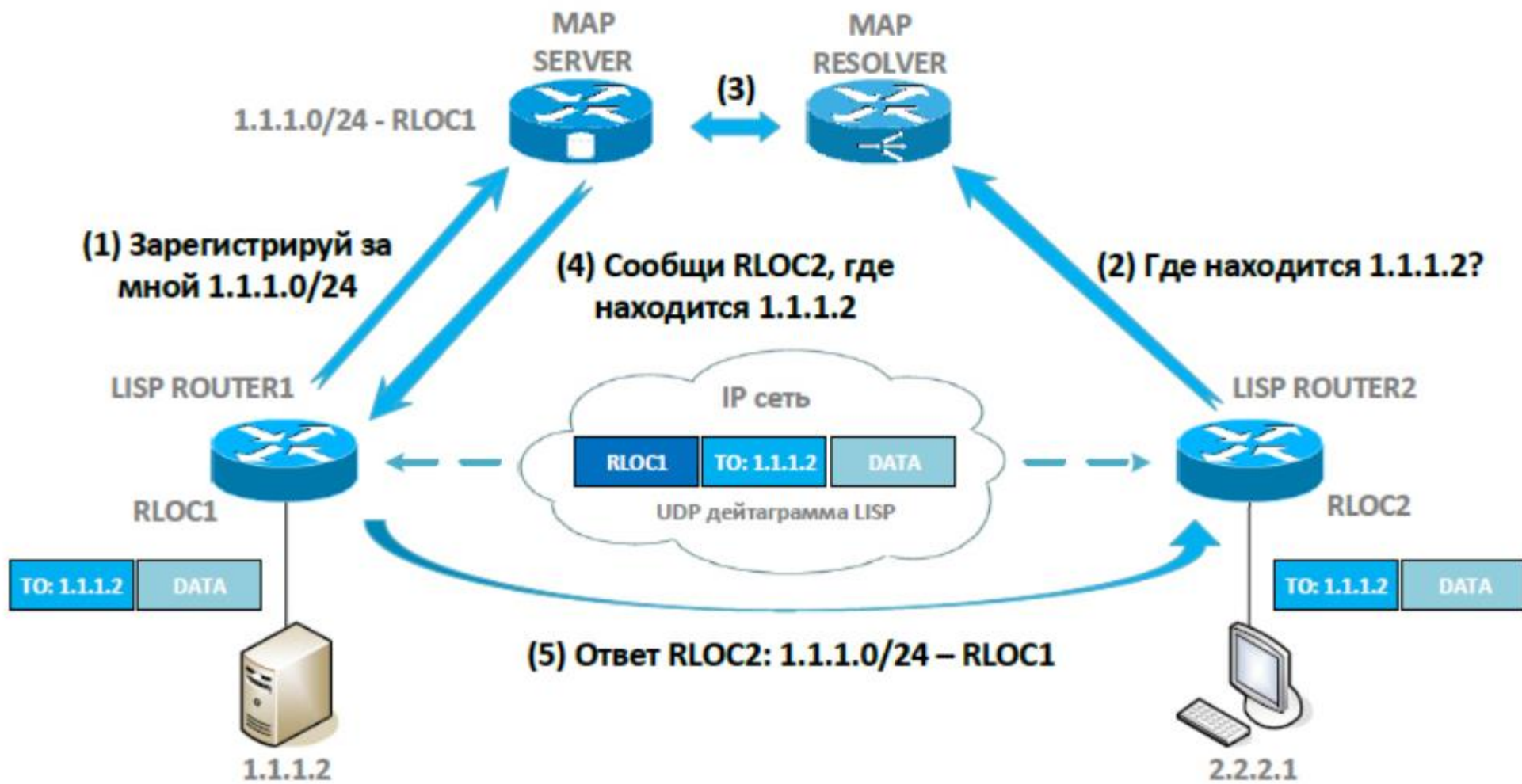


Cisco Locator/ID Separation Protocol – стоит особняком от остальных Overlay технологий, так как помогает не в передаче данных по сети, а только найти нужный нам адрес

Любой адрес в сети с LISP делится на две части:

- адрес сервера (Endpoint Identifier (EID) address)
- адрес устройства, через которое доступен сервер (Route Locator (RLOC) address)

# LISP





# 3.4

VXLAN



# VXLAN

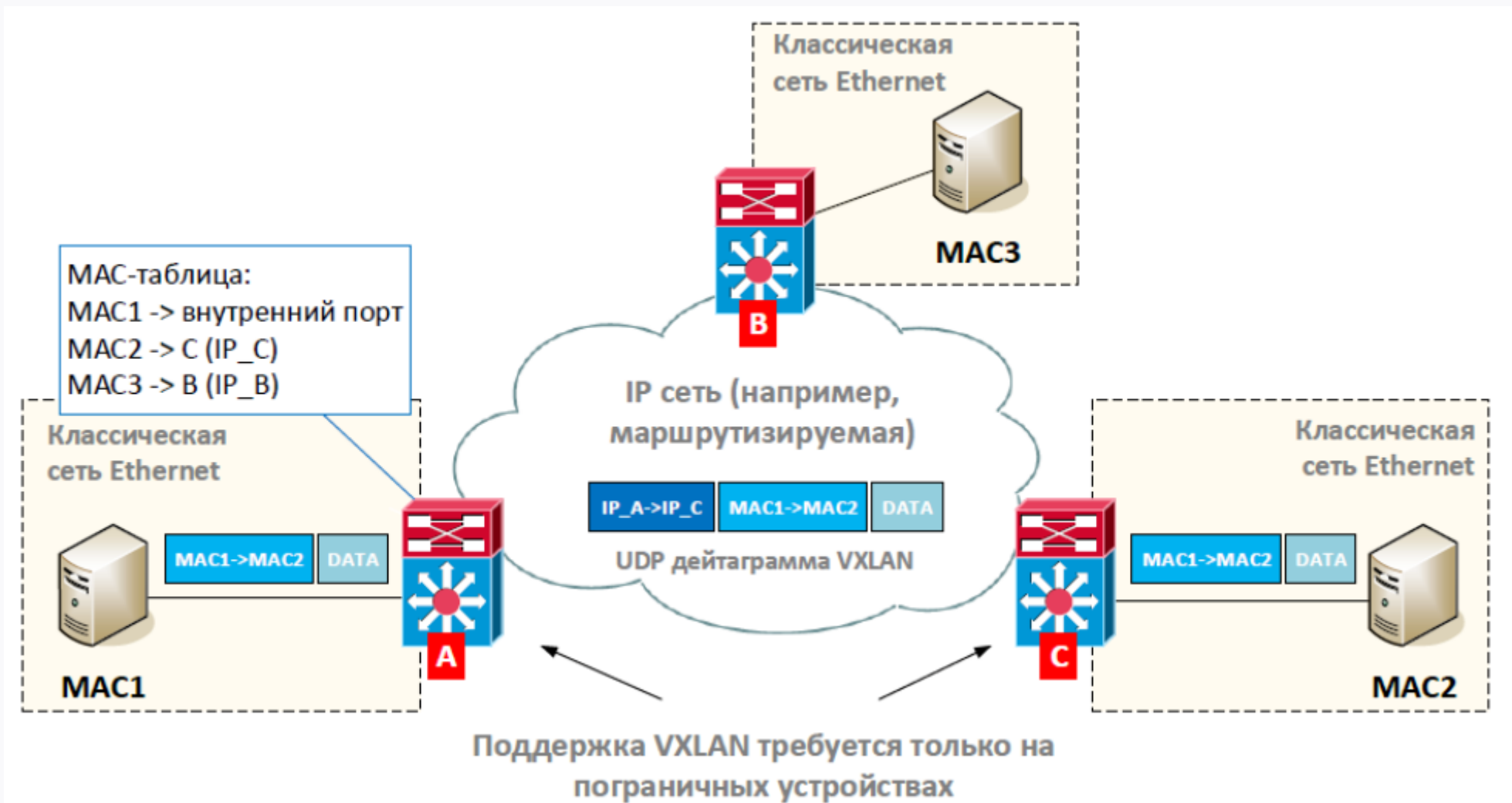
VXLAN – Virtual Extensible LAN, открытая Overlay технология.

Поддерживается практически всеми производителями (Cisco, VMware и т.д.)

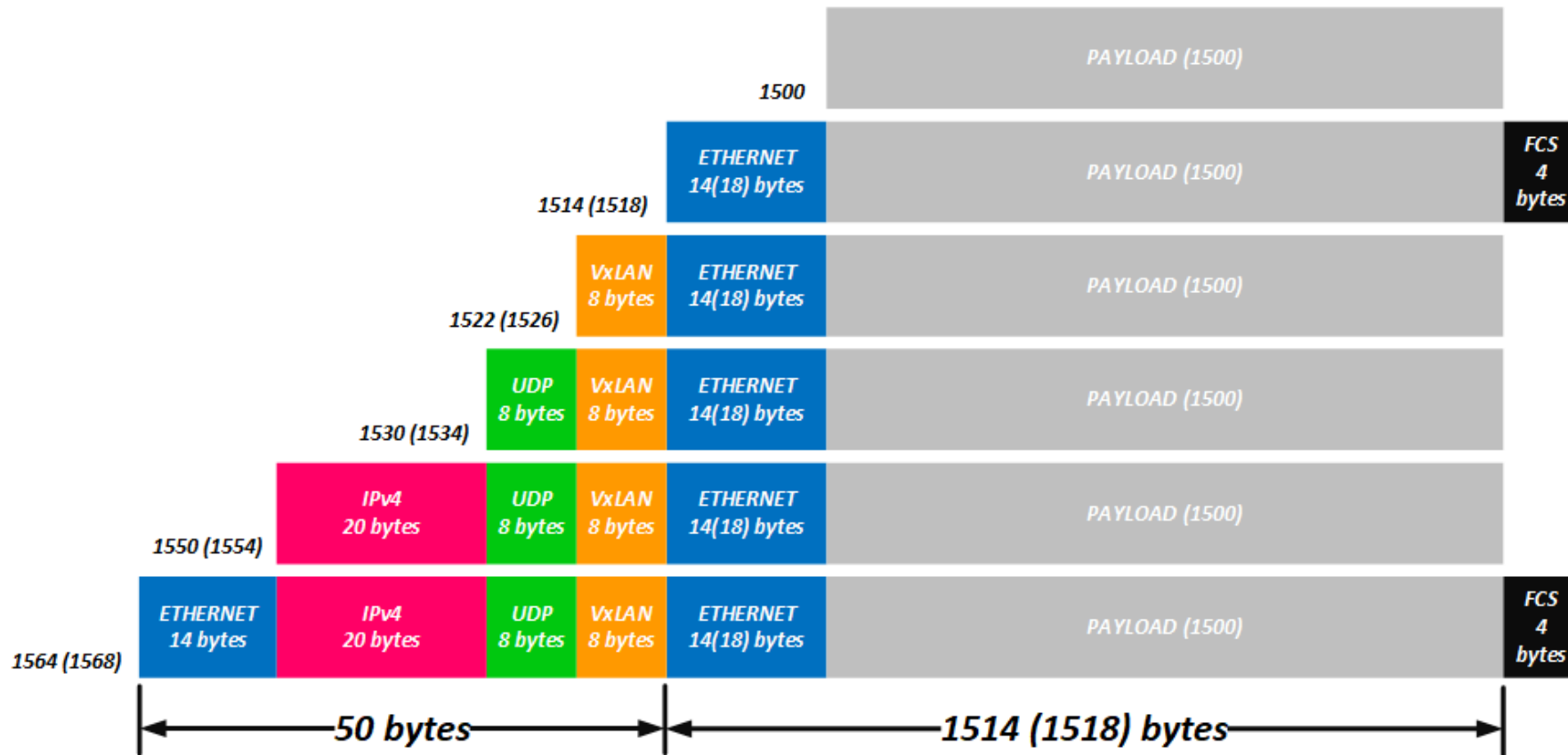
Поддерживает большее 16млн подсетей

Поддерживает L2 поверх IP сети – использует UDP для передачи кадров

# VXLAN



# VXLAN



# VXLAN

## Static:

Вручную прописать соседей VxLAN. Работает только в рамках двух устройств. То есть соединение Point-to-Point. Практически никогда не используется

## Multicast:

Настраивается Multicast группа в рамках которой распространяется информация об IP адресе VTEP (Virtual Tunnel End Point), за которым находится MAC адрес

# VXLAN

MP-BGP EVPN – Multiprotocol Border Gateway Protocol Ethernet Virtual Private Network

Расширение протокола BGP для передача MAC/IP клиента и IP адрес VTEP

Поддерживается на Cisco Nexus

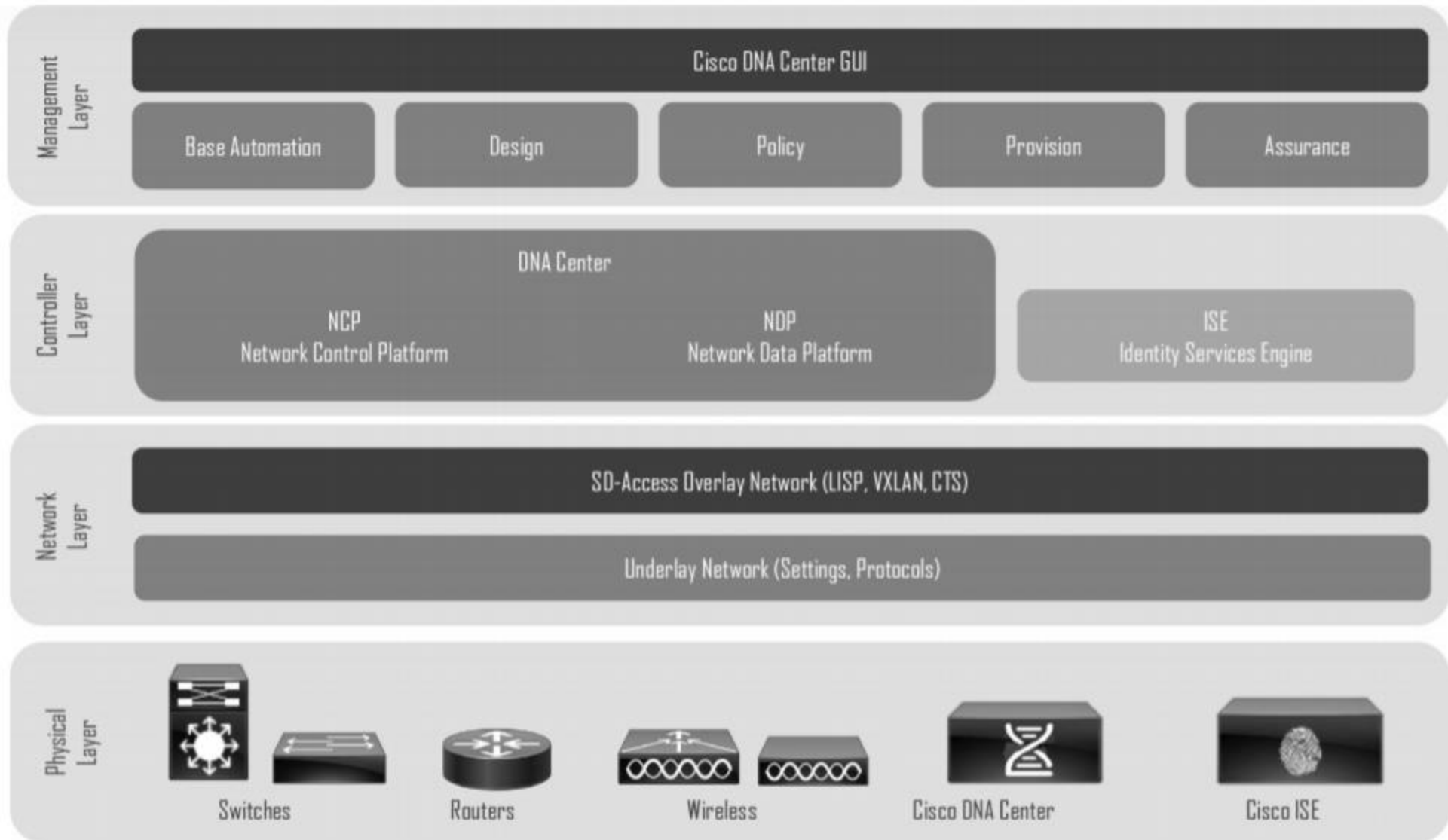


# 4

SD-Access



# SD-Access



Физический уровень:

- Коммутаторы – Cisco Catalyst или Nexus
- Маршрутизаторы – ASR 1000, ISR, CSR
- Контроллеры беспроводных сетей

## Сетевой уровень

Underlay – обеспечивает IP связанность между всеми устройствами. В основе протокол IS-IS

Overlay: Обеспечивает L2 связанность между пользователями, сервисами и т.д.

В основе протоколы VxLAN (Data Plane) и LISP (Control Plane)

Control Plane – Уровень управления сетью:

На данном уровне абстракции работает протокол LISP – распространяется информация о конкретном узле в сети

Data Plane – уровень передачи полезной нагрузки:

На данном уровне абстракции работает протокол VxLAN – данные пользователей инкапсулируются в заголовки VxLAN и передаются по сети на основе информации полученной из Control Plane – LISP.



Заполните, пожалуйста,  
опрос о занятии по ссылке в чате



# До новых встреч!

## Приходите на следующие занятия



**Кулиничев Алексей**

Администратор Сетей

[Santchous42@yandex.ru](mailto:Santchous42@yandex.ru)