The bridge to possible

Фабрика кампусной сети

SD-Access или BGP EVPN VXLAN

Скворчевский Андрей, askvorch@cisco.com
Системный инженер, CCIE #29071
15 июня 2021 года

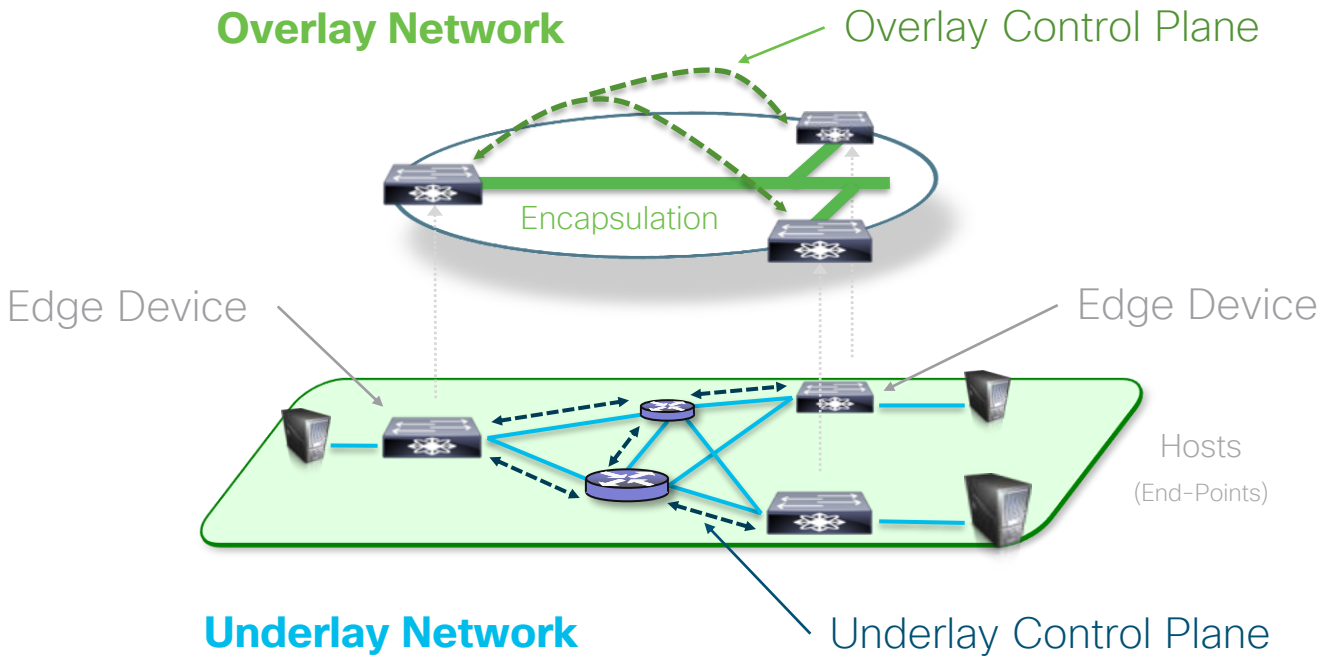
Повестка дня

- Фабрика: зачем нам это нужно
- SD-Access
- BGP EVPN VXLAN
- Заключение

Фабрика

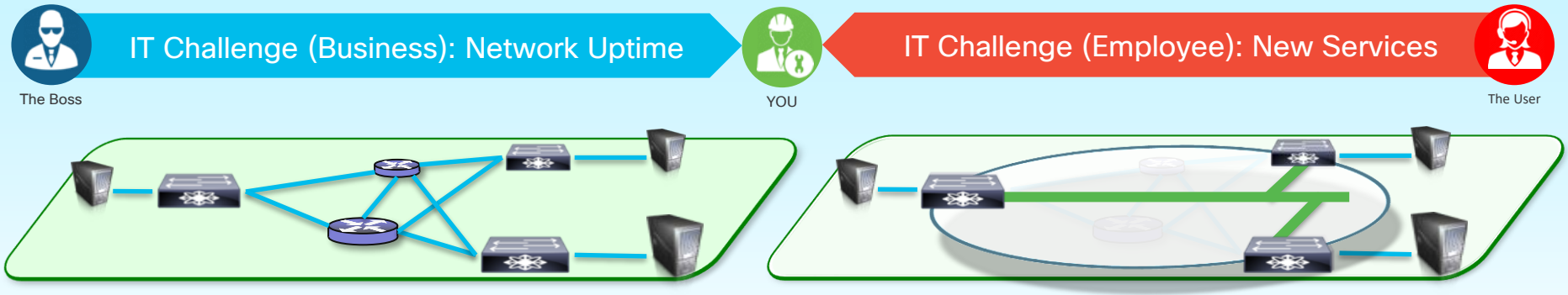
Зачем нам это нужно

Что такое оверлей



Зачем нужен оверлей

Отделить “Сервисную плоскость” от “Транспортной плоскости”



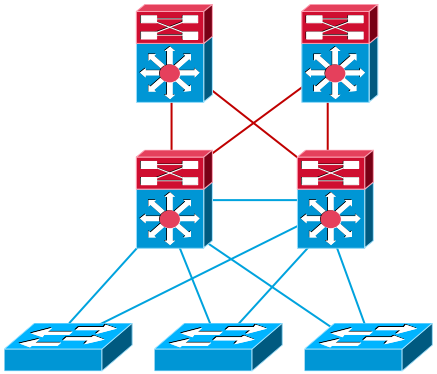
Простая транспортная сеть

- Отказоустойчивость устройств и линков
- Простая и управляемая
- Максимальная пропускная способность
- Максимальная доступность

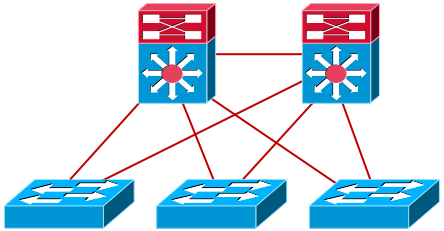
Гибкие виртуальные сервисы

- Мобильность – Привязка Endpoints к Edges
- Сервисы – Предоставляются через оверлей
- Масштабируемость – Определяется протоколом
- Гибкость и программируемость

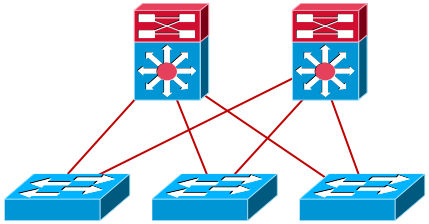
Возможные топологии кампусной сети
Все линки L3 P2P (крайне рекомендуется)



Иерархическая 3-уровневая



Простая 2-уровневая



Spine-Leaf

Почему именно VXLAN?

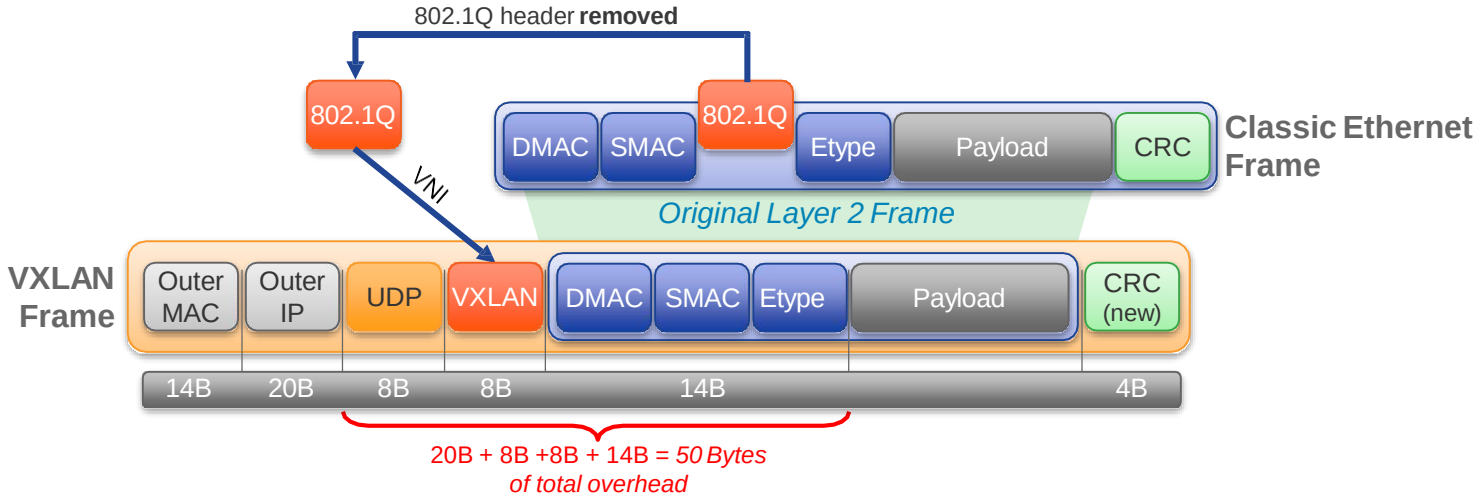
Масштабируемость, сегментация, мобильность конечных устройств

- ✓ Стандартизованный оверлей (RFC 7348)
- ✓ Использование L3 ECMP – полная утилизация всех линков
- ✓ Расширенное до 16M пространство идентификаторов
- ✓ Широкая поддержка производителями оборудования (и ASIC)
- ✓ Интеграция физической и виртуальной сетей

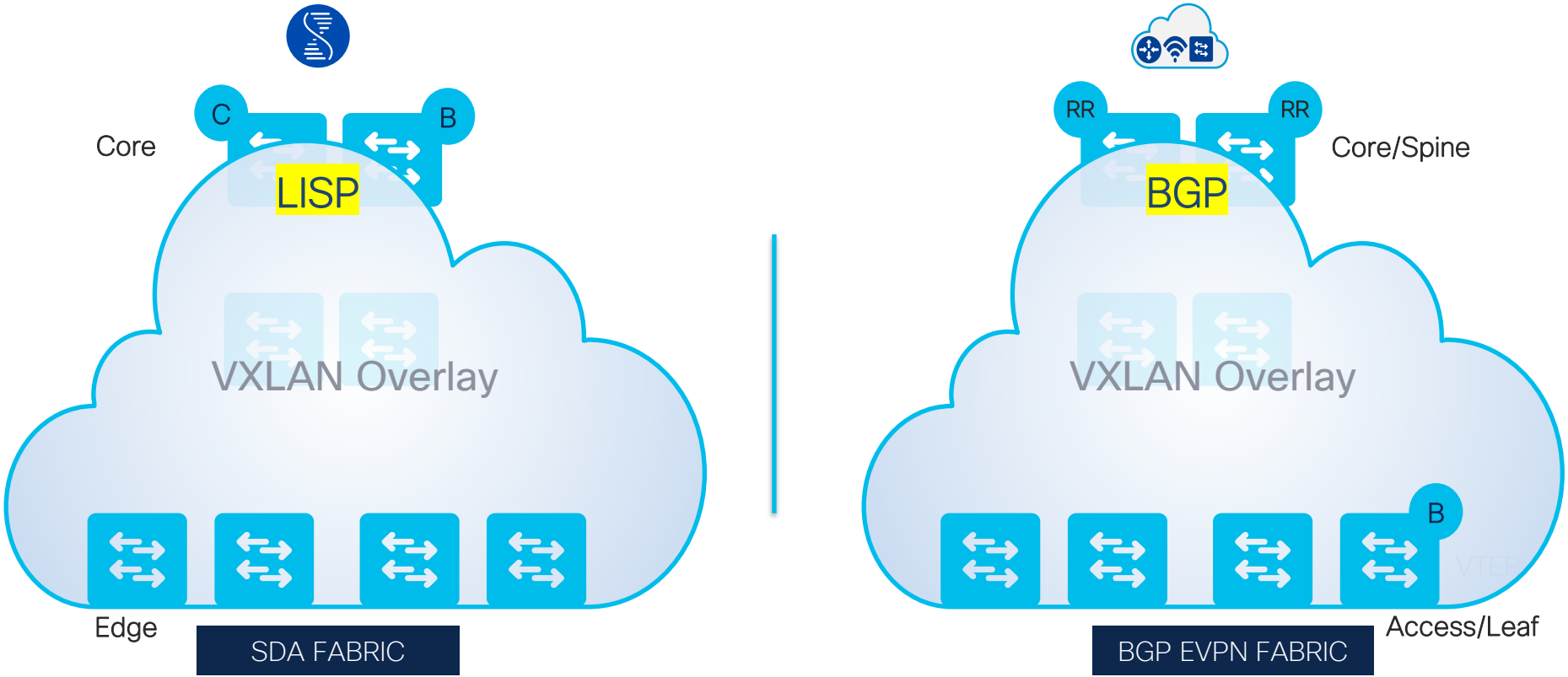
VXLAN: общая информация

- Традиционный VLAN кодируется 12 битами (802.1Q tag)
  - Максимальное количество сегментов не более 4096 (на практике даже меньше)

- VXLAN использует поле VNI, которое кодируется 24 битами
  - Поддержка ~16M сегментов
- VXLAN Network Identifier (VNI/VNID) – это часть заголовка VXLAN пакета



SDA и BGP EVPN: сходства и различия

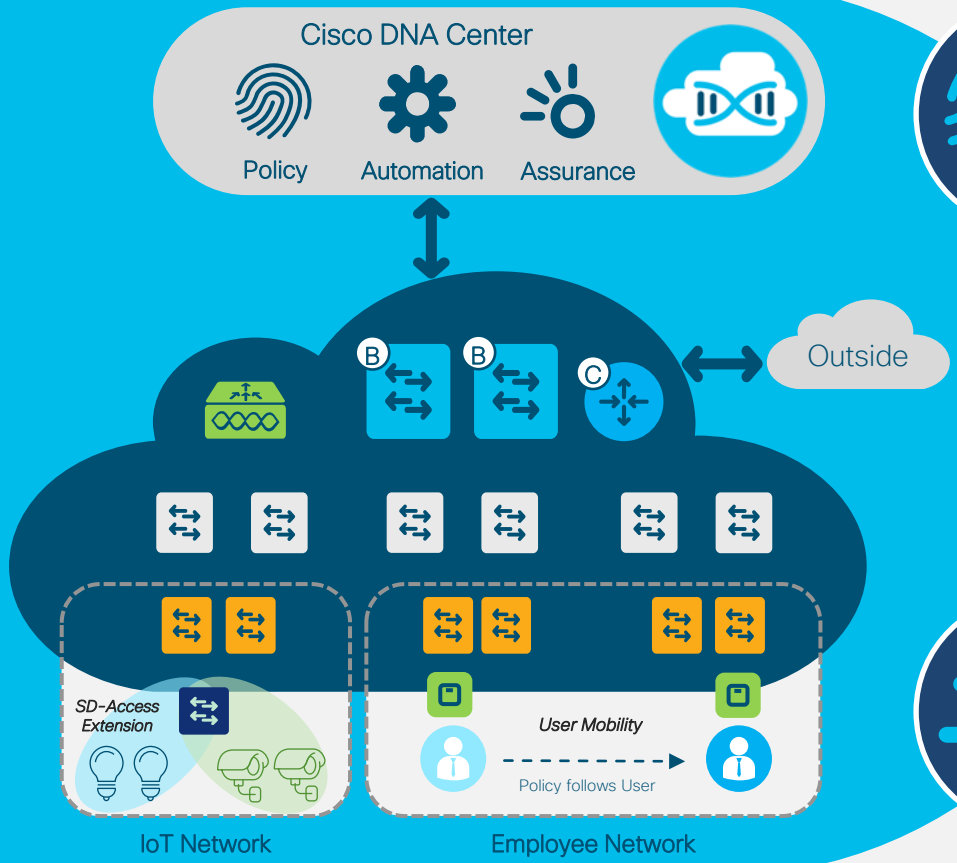


SD-Access

Кампусная фабрика «под ключ»

Cisco Software Defined Access

Основа Intent-Based Network



Политика и сегментация на основании сущности

Больше нет нужды в жесткой привязке к VLAN и IP-адресу

Автоматизированная фабрика сети

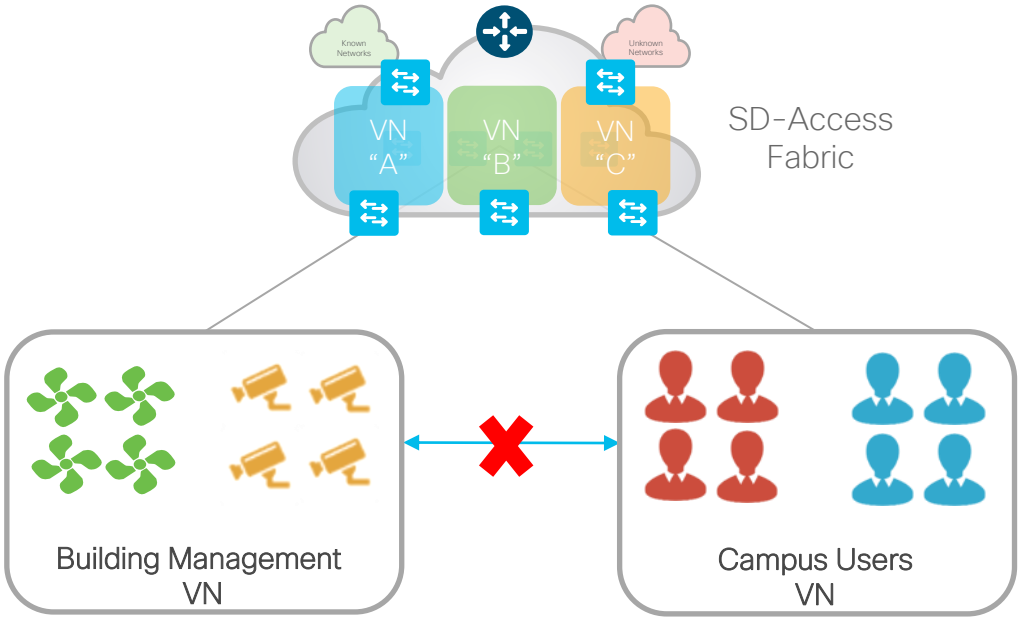
Единая фабрика проводной и беспроводной сети с автоматизацией

Наблюдаемость и телеметрия

Постоянный анализ пользователей и приложений

Политики SD-Access

Двухуровневая иерархия- Макросегментация

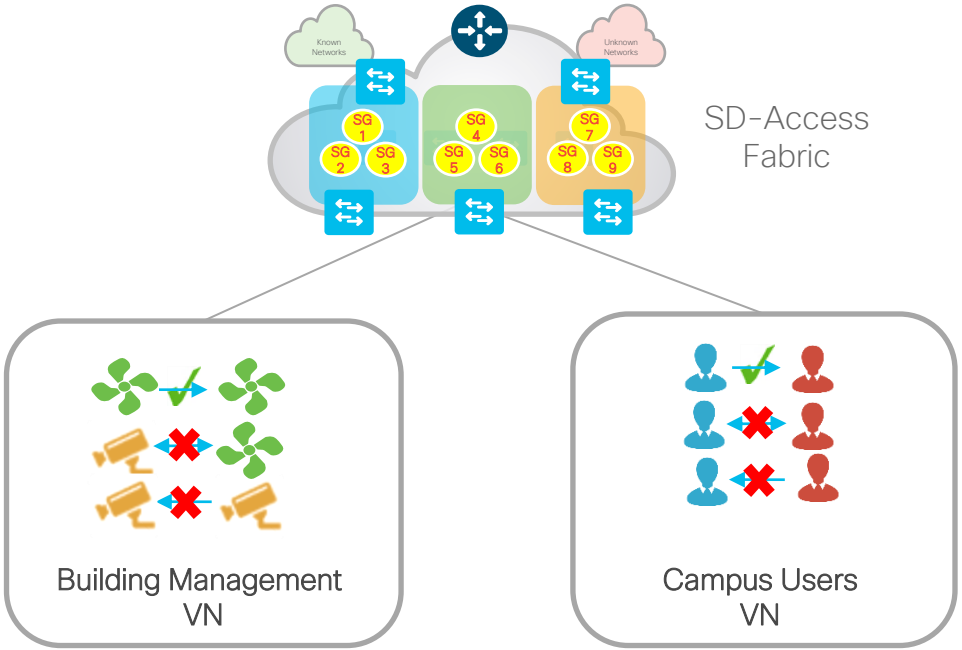


Virtual Network (VN)

Первый уровень сегментации обеспечивает полную изоляцию между множественными виртуальными сетями, построенными поверх одной физической инфраструктуры

Политики SD-Access

Двухуровневая иерархия – Микросегментация

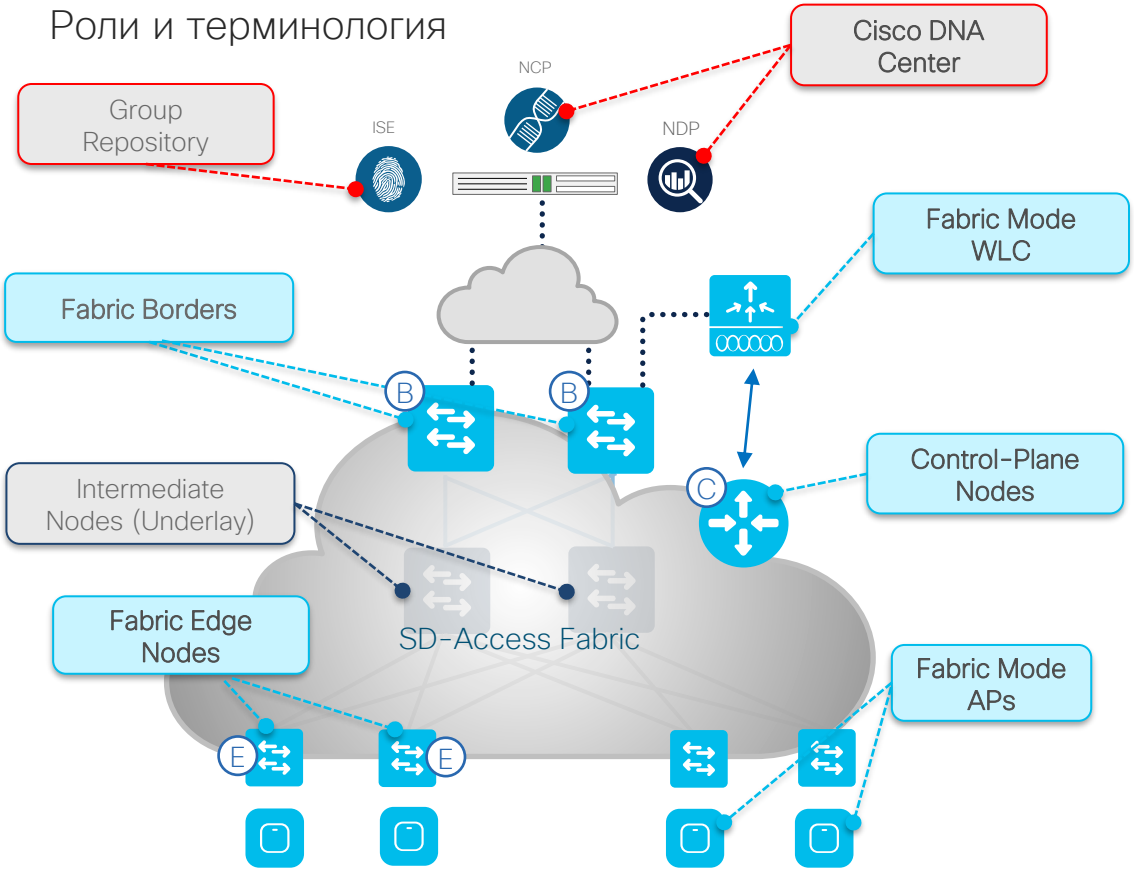


Scalable Group (SG)

Второй уровень сегментации обеспечивает контроль доступа на основе ролей между группами в рамках одной VN. Позволяет разделять пользователей исходя из выполняемых ими функций

Архитектура фабрики SD-Access

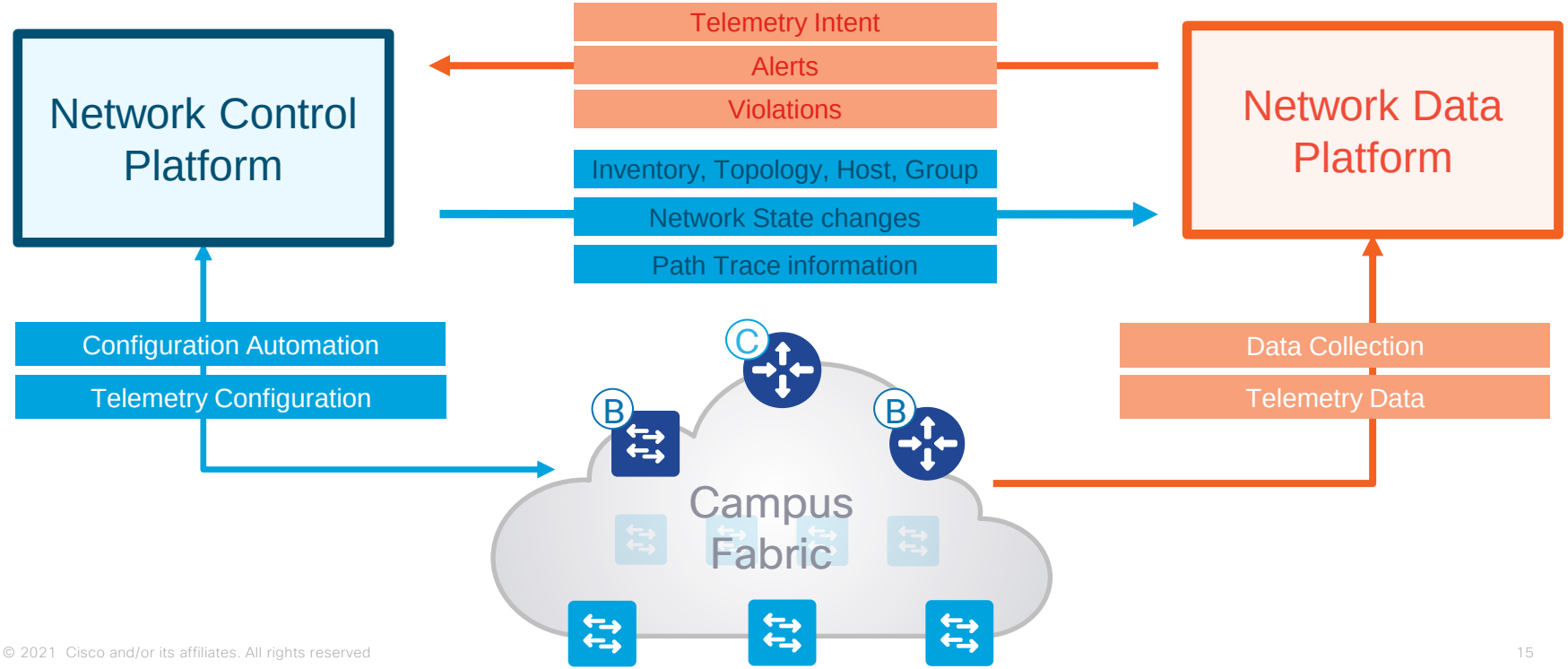
Роли и терминология



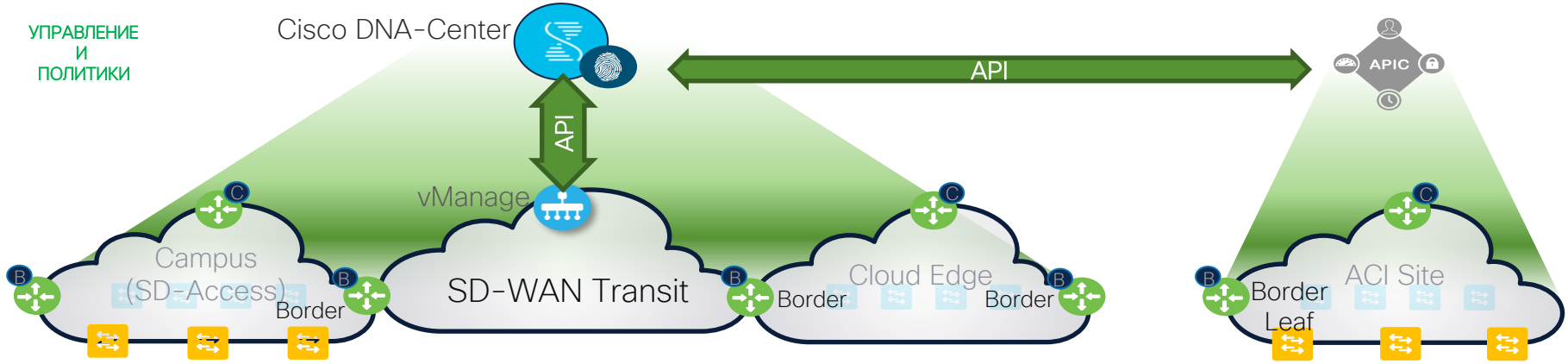
- **Cisco DNA Center** – Контроллер SDN сети с графическим интерфейсом пользователя. Осуществляет управление и мониторинг сети
- **Group Repository** – Сервис идентификации для контроля пользователей и устройств, присвоения меток и привязки политик
- **Control-Plane Nodes** – Система привязки конечных устройств к Edge узлам. Известна также как Host Tracking DB (HTDB)
- **Border Nodes** – Устройства фабрики (например, Core), которые подключают фабрику к внешним L3 сетям
- **Edge Nodes** – Устройства фабрики (Access), которые подключают к фабрике конечные устройства
- **Fabric Mode Wireless Controller** – Интегрированный в фабрику Wireless Controller (WLC)
- **Fabric Mode APs** – Интегрированные в фабрику ТД. Беспроводной трафик сразу инкапсулируется в VXLAN

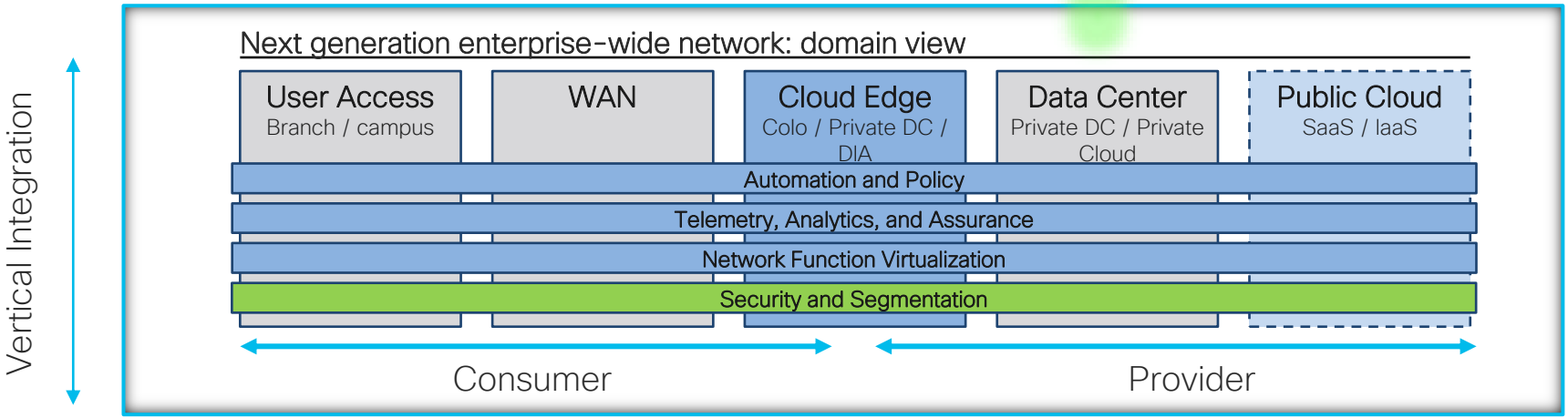
Cisco DNA Center

Автоматизированная настройка и телеметрия



Корпоративная сеть следующего поколения



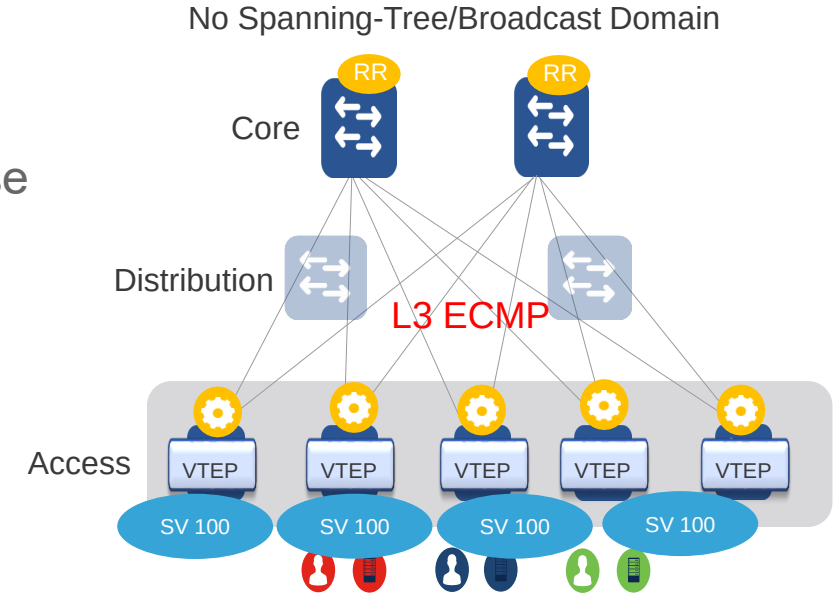


BGP EVPN VXLAN

Решение для самостоятельной интеграции

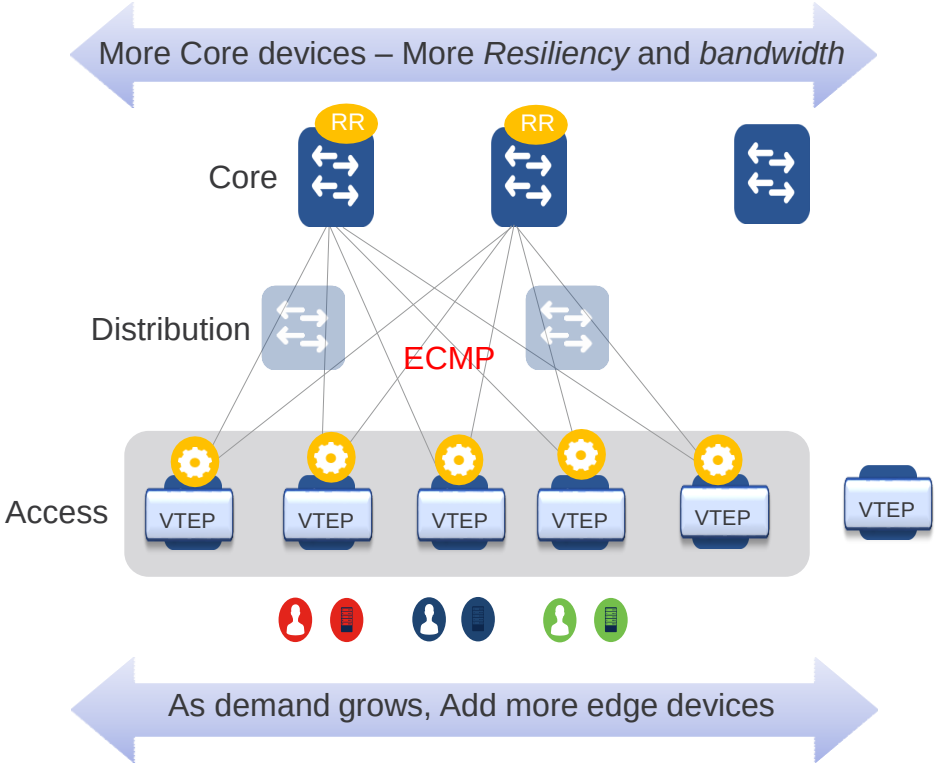
Почему EVPN?

- Любая подсеть на любом устройстве
- L3 ECMP и утилизация всех линков
- BGP Control Plane
- Расширяемость и отказо-устойчивость
- Распределенный шлюз на всех устройствах доступа

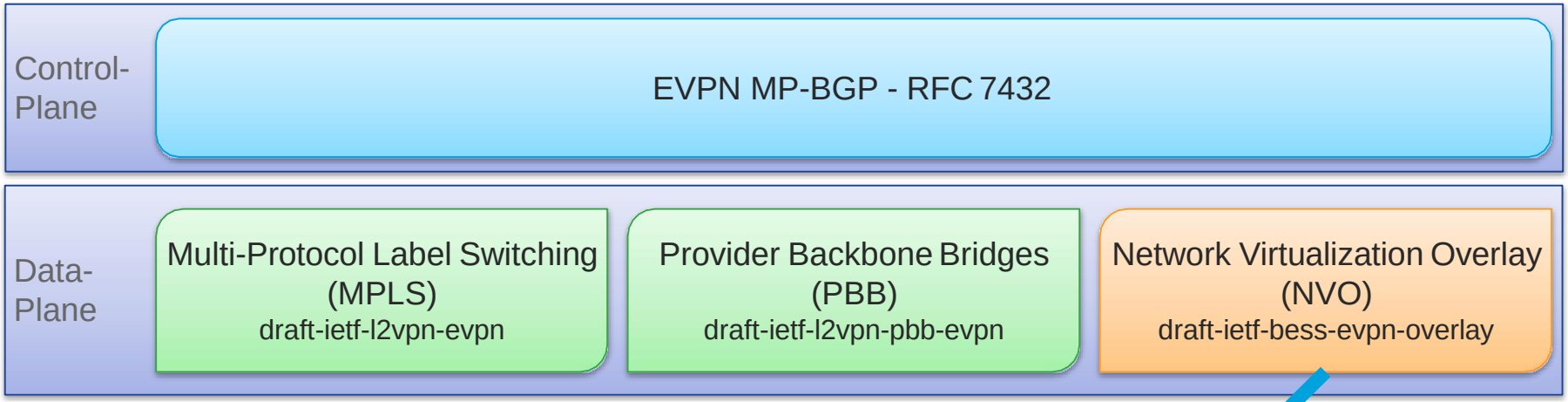


Масштабируемость

- Размеры фабрики: от сотен до десятков тысяч портов 1/10G
- Гибкость компоновки:
  - Любые типы интерфейсов
  - Любая плотность портов
  - Любой уровень переподписки
- Простая масштабируемость
  - Возможность добавлять устройства любого типа (Spine/Leaf/Border) по мере необходимости



EVPN – Ethernet VPN



- EVPN over NVO Tunnels (ie VXLAN)
- Provides Layer-2 and Layer-3 Overlays over simple IP Networks

Что нам дает VXLAN вместе с BGP EVPN?

- Стандартизованный Overlay (VXLAN) со стандартизованным Control-Plane (BGP)
- Распространение Layer-2 MAC и Layer-3 IP информации через Control-Plane (BGP)
- Передача трафика на основании информации Control-Plane (минимизация широковещательных запросов)
- Integrated Routing/Bridging (IRB) для оптимальной передачи трафика в Overlay
- Масштабируемость и Multi-Tenancy

Что есть что

VXLAN

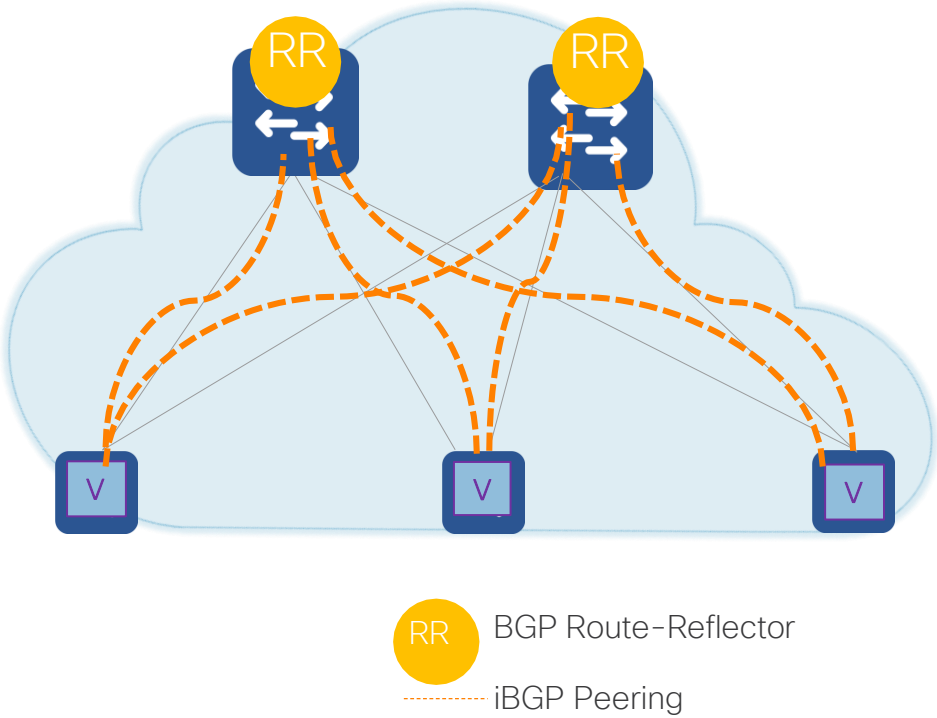
- Standards based Encapsulation
- RFC 7348
- Uses UDP-Encapsulation
- Transport Independent
- Layer-3 Transport (Underlay)
- Flexible Namespace
- 24-bit field (VNID) provides ~16M unique identifier
- Allows Segmentations

EVPN

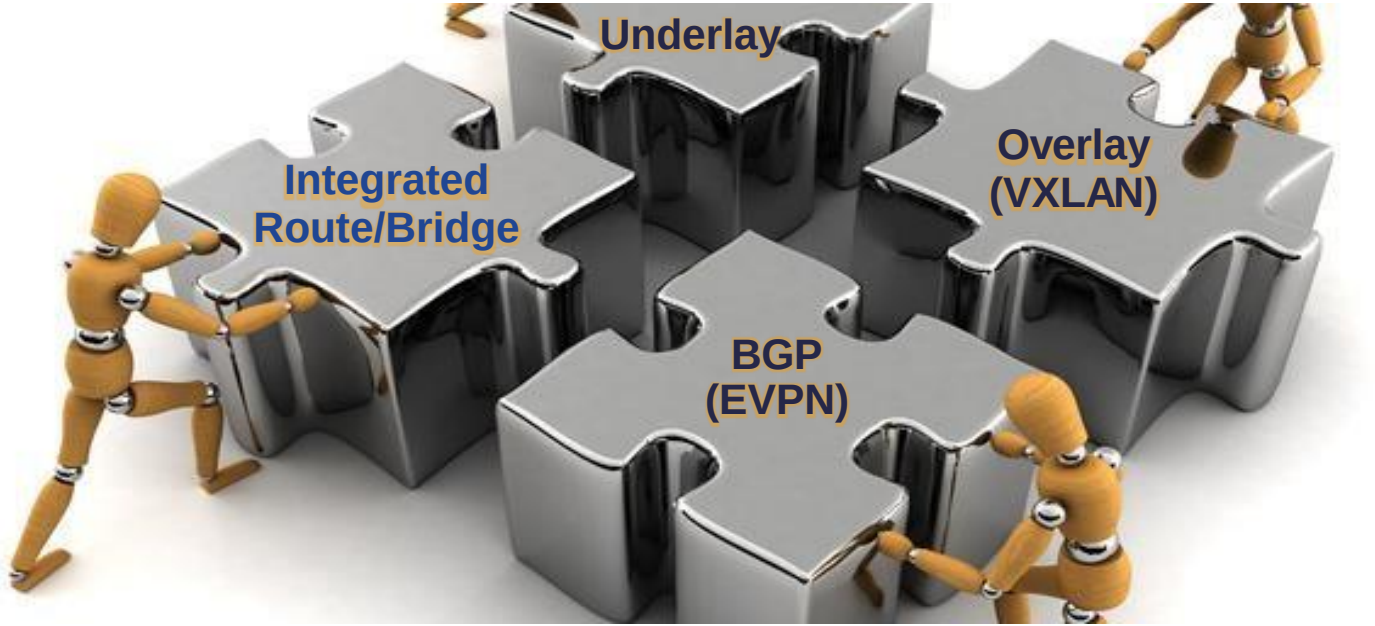
- Standards based Control-Plane
- RFC 8365 (and RFC 7432)
- Uses Multiprotocol BGP
- Uses Various Data-Planes
- VXLAN (EVPN-Overlay), MPLS, Provider Backbone (PBB)
- Many Use-Cases Covered
- Bridging, MAC Mobility, First-Hop & Prefix Routing, Multi-Tenancy (VPN)

Multiprotocol BGP (MP-BGP)

- Стандартизованное расширение протокола BGP (RFC 4760)
- VPN Address-Family:
  - Разные типы адресных пространств (VPNv4, VPNv6, L2VPN EVPN, MVPN)
- Вся информация передается через единую сеть BGP маршрутизаторов

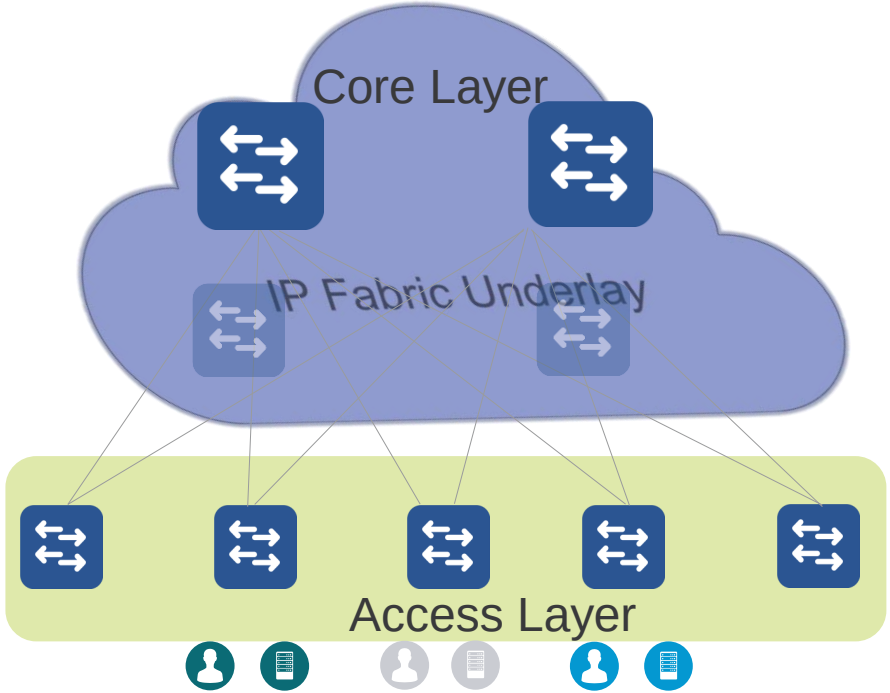


Собираем все компоненты вместе!

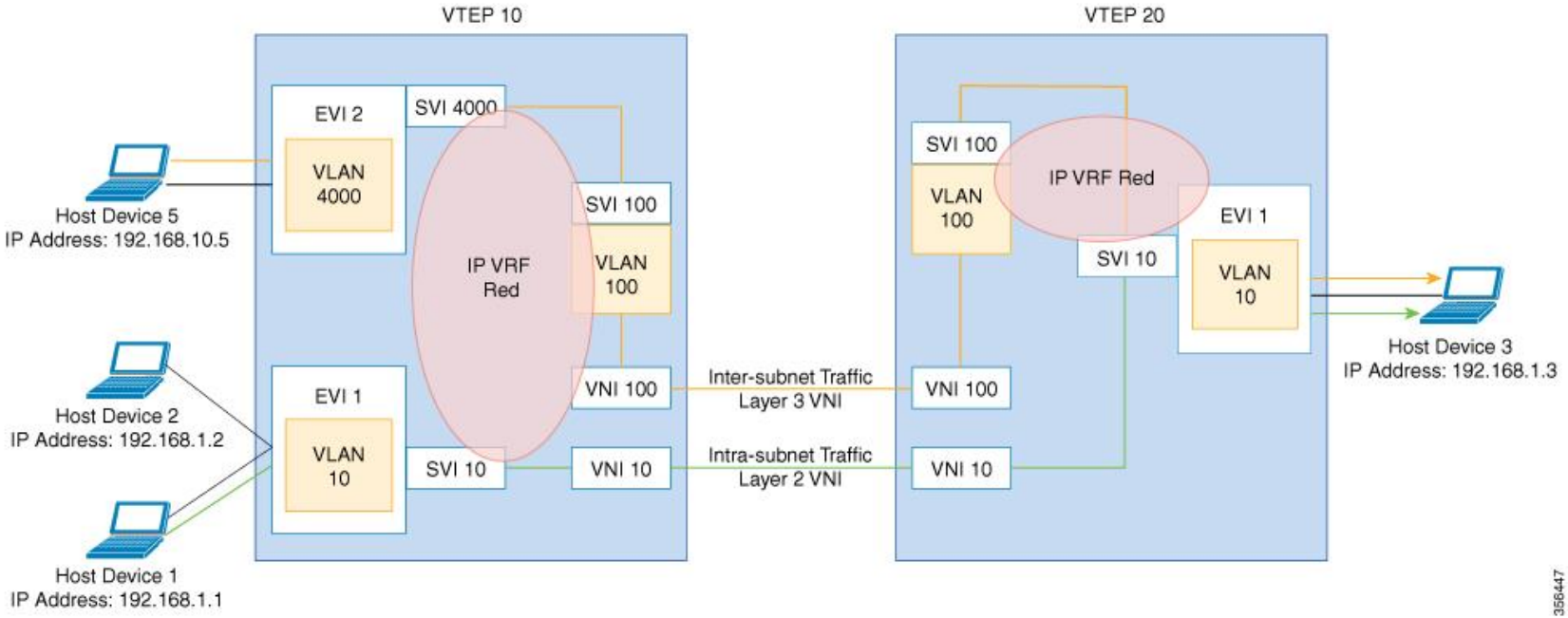


Особенности реализации

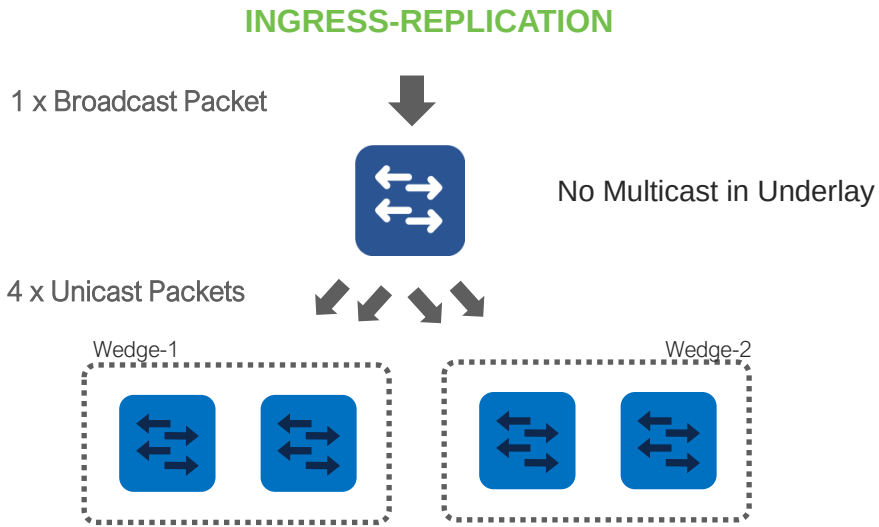
- Underlay routing protocol
  - ISIS, OSPF, BGP
- Организация BGP
  - Одна AS, две AS, много AS
- Механизм обработки BUM трафика
  - Ingress-replication, multicast-replication
- Конфигурация VNI
  - Consistent, scoped

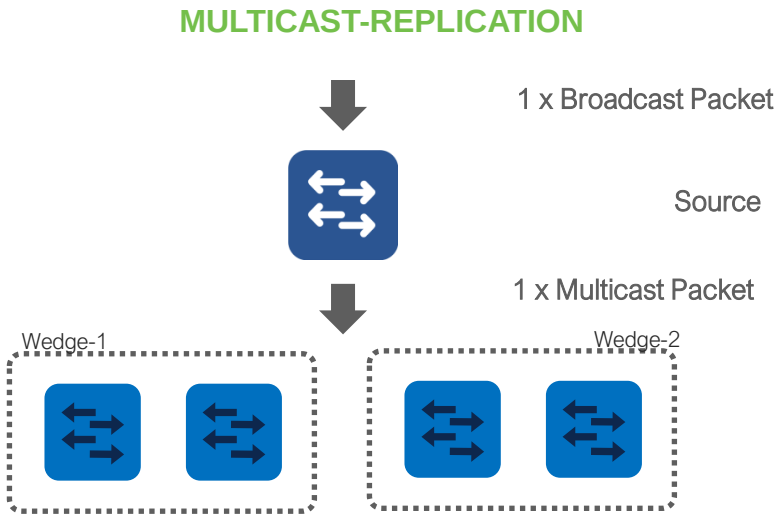


Коммутация и маршрутизация



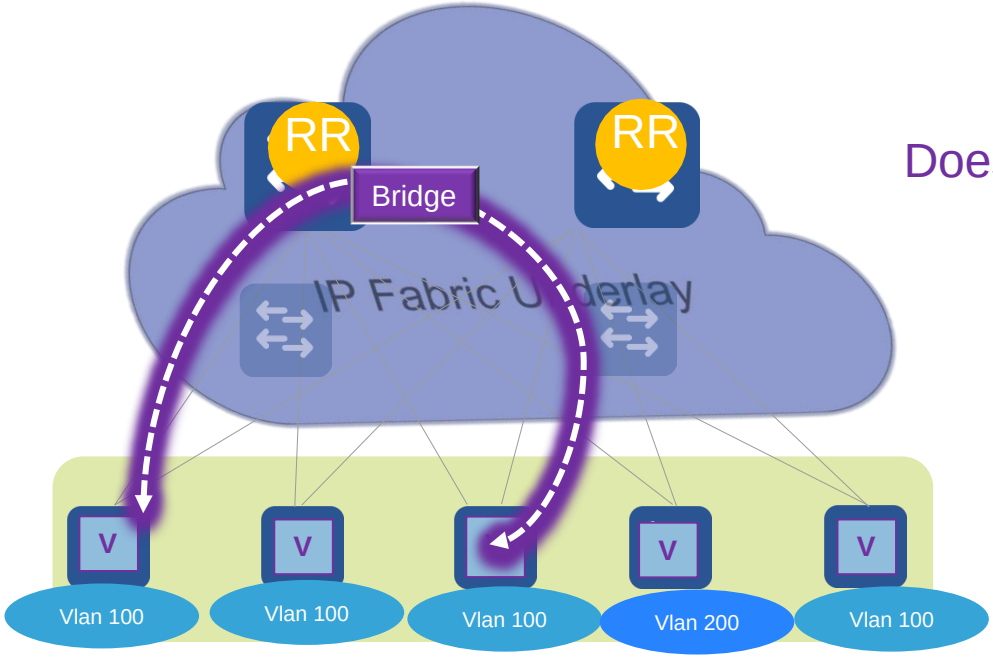
Механизмы BUM репликации





- Два механизма обработки **B**roadcast, **U**nknown Unicast and Link-Local **M**ulticast (BUM):
  - Ingress-Replication – Конвертация каждого BUM пакета в множество Unicast пакетов и отправка на каждый VTEP
  - Multicast-Replication – Конвертация каждого BUM пакета в один Multicast пакет и отправка его в Underlay сеть
- Вариант Multicast-Replication увеличивает масштабируемость и снижает нагрузку

Layer-2 Multi-Tenancy

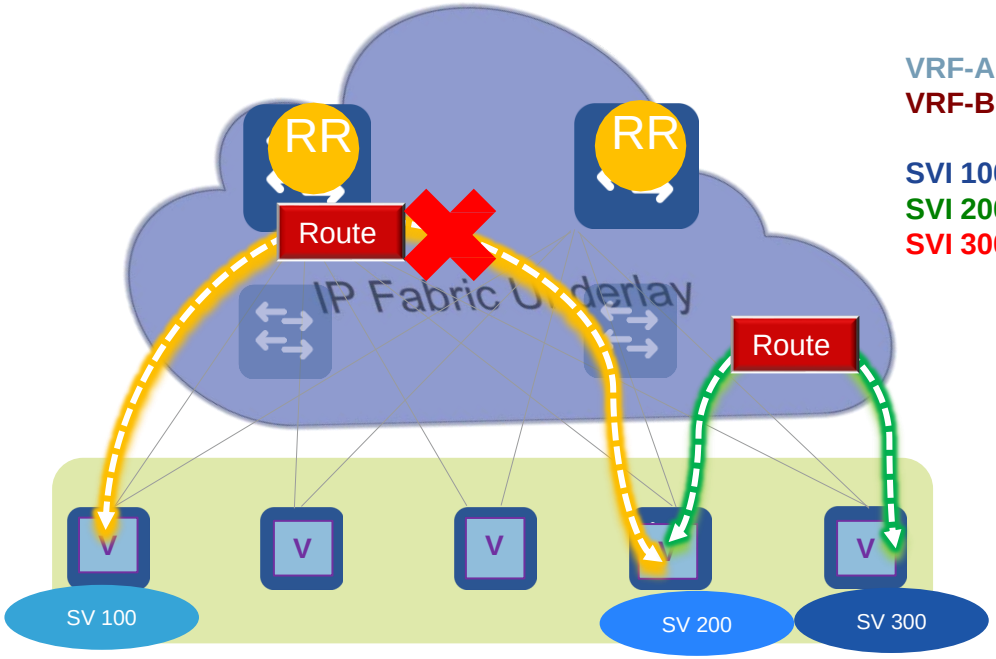


Does not require a VRF

Host1
MAC: AA:AA:AA:AA:AA:AA
IP: 192.168.1.11
VLAN 100
VXLAN VNI 30001

Host3
MAC: CC:CC:CC:CC:CC:CC
IP: 192.168.1.33
VLAN 100
VXLAN VNI 30001

Layer-3 Multi-Tenancy



VRF-A (VNI 50001)
VRF-B (VNI 50002)

SVI 100, Gateway IP: 192.168.1.1 (VRF-A)
SVI 200, Gateway IP: 172.26.200.1 (VRF-B)
SVI 300, Gateway IP: 10.10.10.1 (VRF-B)

Host1
IP: 192.168.1.11 **(VRF A)**
VLAN 100
VXLAN VNI 50001

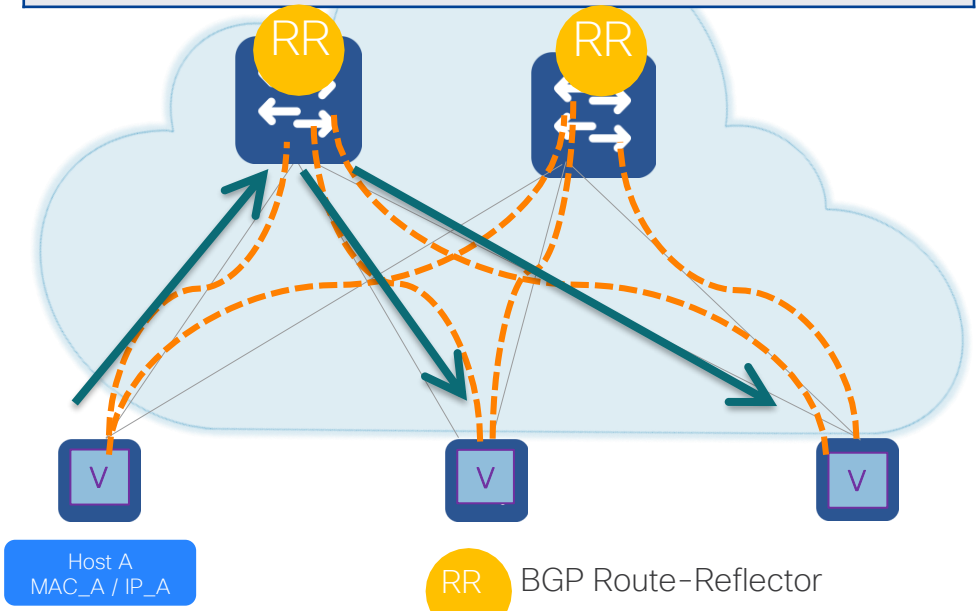
Host3
IP: 172.26.200.11 **(VRF B)**
VLAN 200
VXLAN VNI 50002

Host2
IP: 10.10.10.22 (VRF B)
VLAN 300
VXLAN VNI 50002

Изучение MAC/IP адресов
“MAC or MAC/IP host Advertisement (Route-Type 2)”

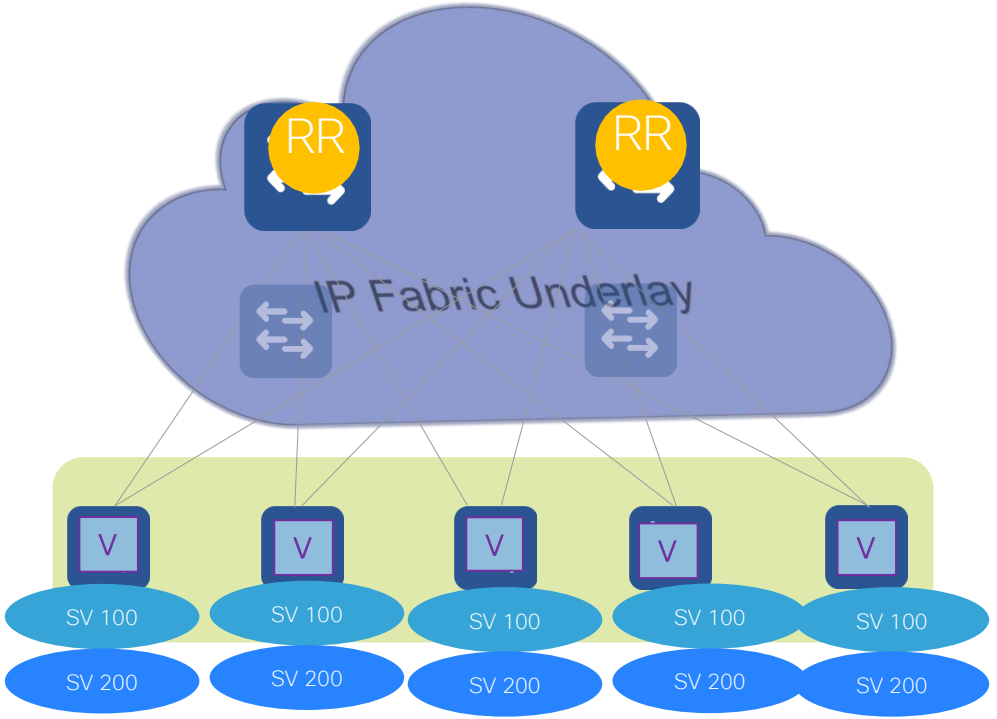
- Host “A” attaches to Edge Device (VTEP)
- VTEP V1 advertises Host “A” reachability information
  - MAC and L2VNI [mandatory]
  - IP and L3VNI [optional]
- Additional Attributes advertised
  - MPLS Label 1 (Layer-2 VNI)
  - MPLS Label 2 (Layer-3 VNI)
  - Extended Communities

Route Type	MAC, IP	L2VNI	Layer-3 VNI (“VRF”)	NH	Encap	Seq
2	MAC_A, IP_A	30001	50001	IP_V1	8:VXLAN	0



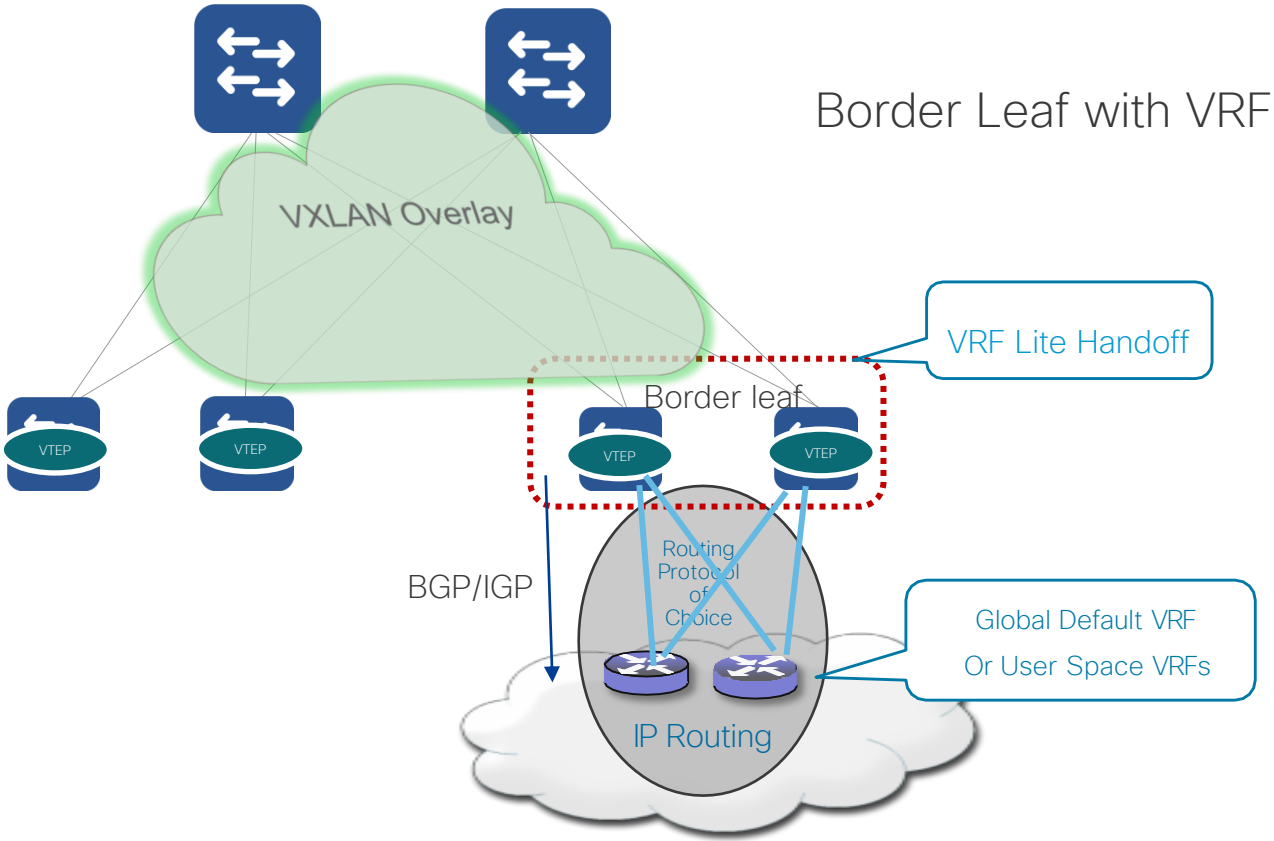
Distributed IP Anycast Gateway

- Распределенная Inter-VXLAN маршрутизация на уровне доступа (Edge)
  - Все коммутаторы доступа разделяют одни и те же IP и MAC адреса шлюза для конкретной подсети
- Шлюз всегда активен
  - Никаких FHRP протоколов, hello, heartbeat и т. д.

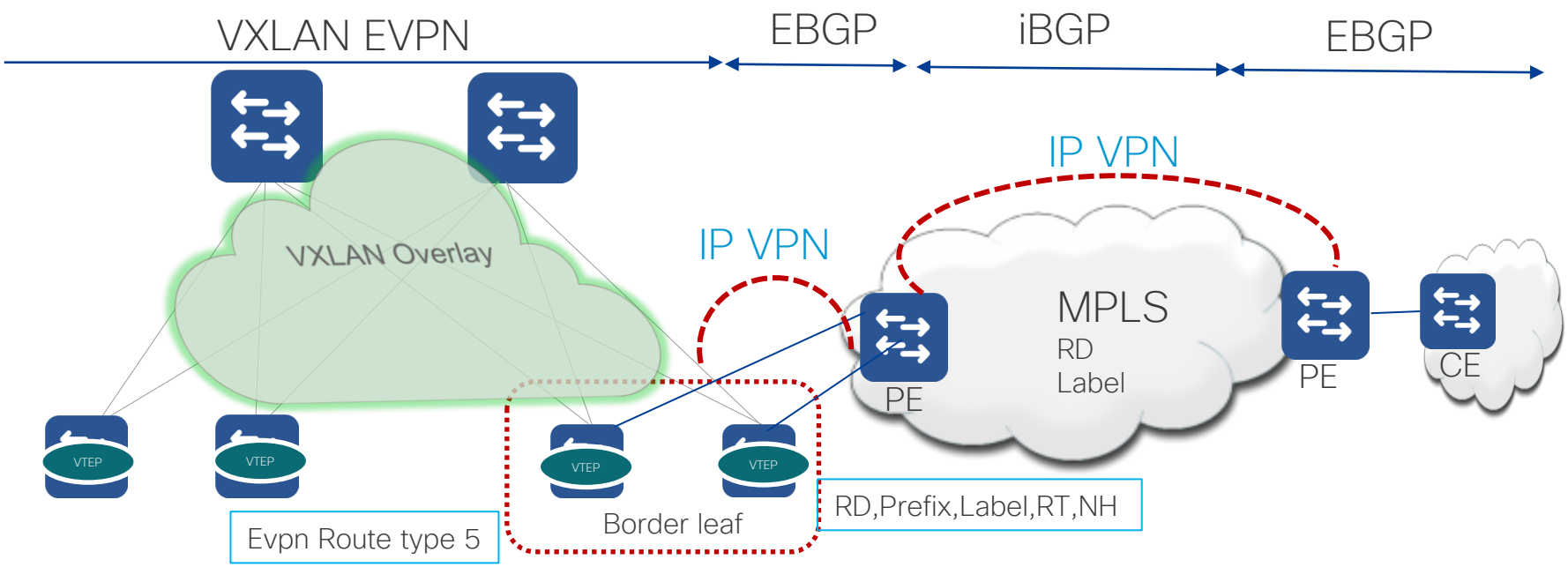


SVI 100, Gateway IP: 192.168.1.1, Gateway MAC: AG:AG:AG:AG:AG:AG
SVI 200, Gateway IP: 10.10.10.1, Gateway MAC: AG:AG:AG:AG:AG:AG

Маршрутизация фабрики с внешними сетями

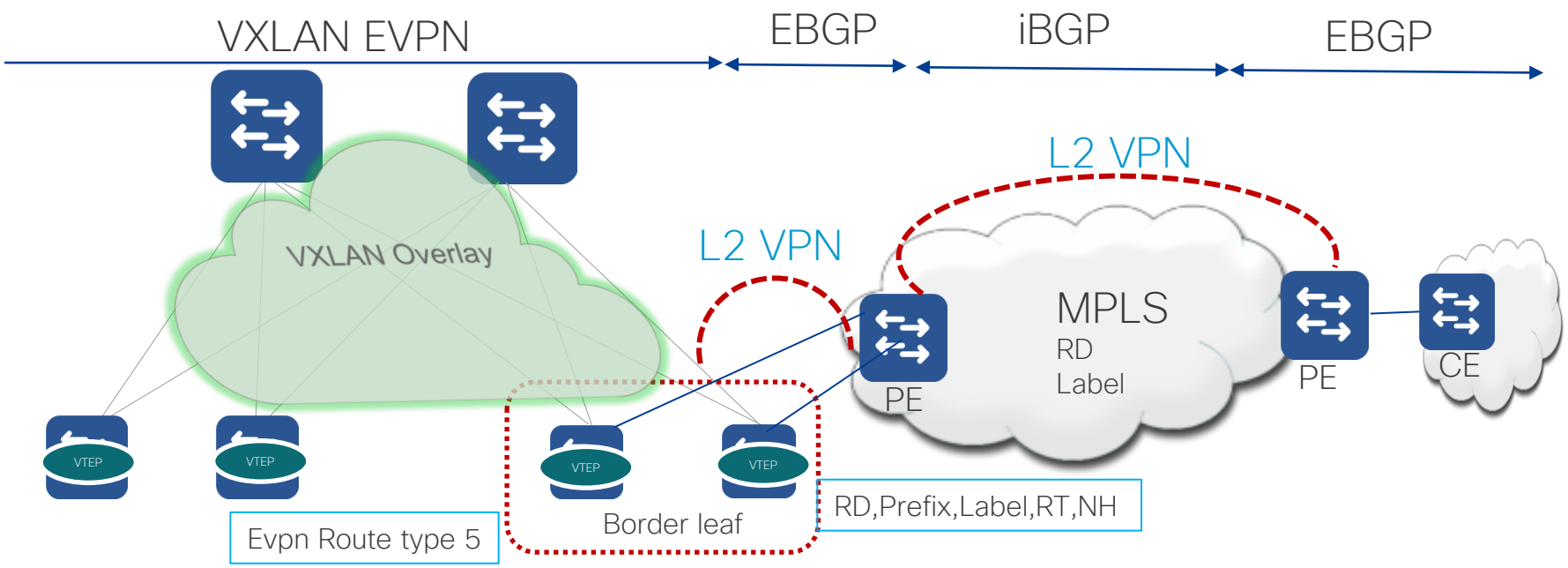


L3VPN Handoff



Single Box Solution – Border Leaf interconnecting EVPN with MPLS L3VPN

L2VPN Handoff



Single Box Solution – Border Leaf interconnecting EVPN with VPLS

Catalyst 9K – Модели и роли

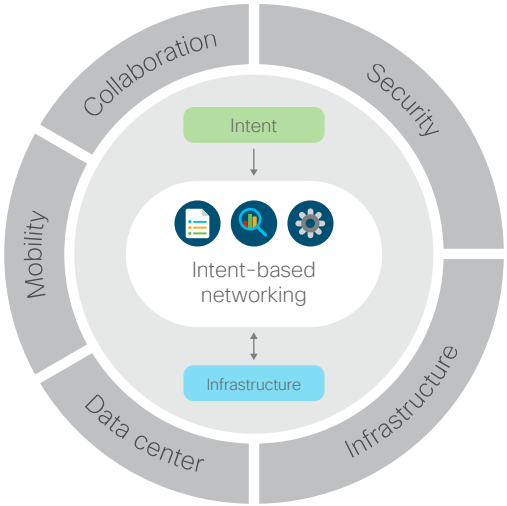
Catalyst 9K	Role
Catalyst 9200/L	Unsupported
Catalyst 9300/L	Leaf | Spine
Catalyst 9400	Leaf | Spine
Catalyst 9500	Leaf | Spine
Catalyst 9500H*	Leaf | Spine | Border
Catalyst 9600	Leaf | Spine | Border

* Catalyst 9500H – это модели Catalyst 9500 на базе ASIC UADP 3.0 (C9500-32C, -32QC, -24Y4C, -48Y4C)

Заключение

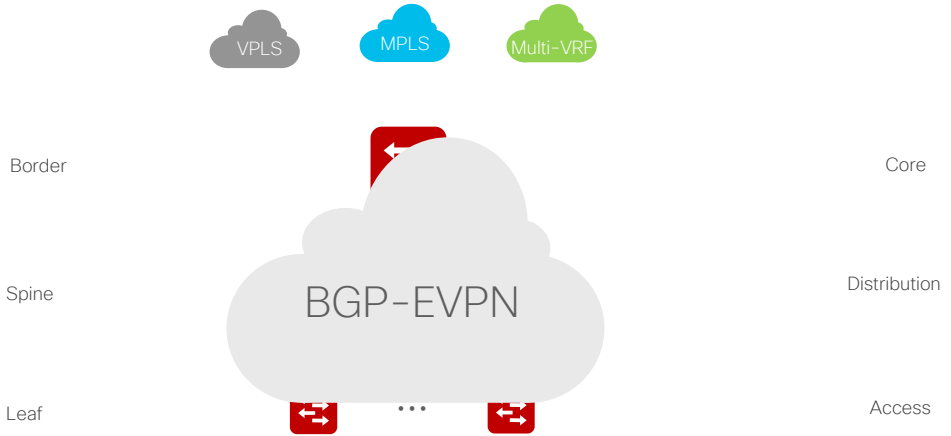
Выбор архитектуры кампусной фабрики

SD-Access



- Лучшая в энтерпрайз-классе архитектура, **обеспечивающая мобильность и безопасность пользователей**
- Встроенная автоматизация и аналитика благодаря **Cisco DNA Center**
- Изначальная интеграция беспроводной инфраструктуры **и общие политики для проводных и беспроводных пользователей**

BGP EVPN



- Решение на базе индустриальных стандартов **для интеграции с устройствами сторонних производителей**
- Решение для **Brownfield интеграций** – MPLS, VPLS, Multi-VRF, GRE.
- **Единый Overlay** для сетей кампуса и датацентра
- **Провиженинг и автоматизация – ответственность Заказчика (DIY)**

Итог

- SD-Access
  - Полностью готовое к внедрению и эксплуатации решение
  - DNA Center – основа функционала SD-Access фабрики
  - Непрерывное развитие решения силами и ресурсами Cisco

- BGP EVPN VXLAN
  - Открытые стандарты и возможность интеграции с любым другим оборудованием
  - Возможность реализовать принципиально иной функционал, чем SD-Access
  - Вероятно потребуются дополнительные компоненты (автоматизация, мониторинг)
  - Дальнейшее развитие решения своими силами

The bridge to possible