Workshop Secure Automated Campus

Москва, 11 апреля 2019 г.

Что нас ждет в ближайшие полтора часа

Часть 1: Что такое Extreme Automated Campus

- Общие сведения
- Базовые сервисы Fabric Connect
- Дополнительные сервисы: DVR, PIM Gateway, VXLAN Gateway
- Аппаратные платформы для построения фабрики

Перерыв

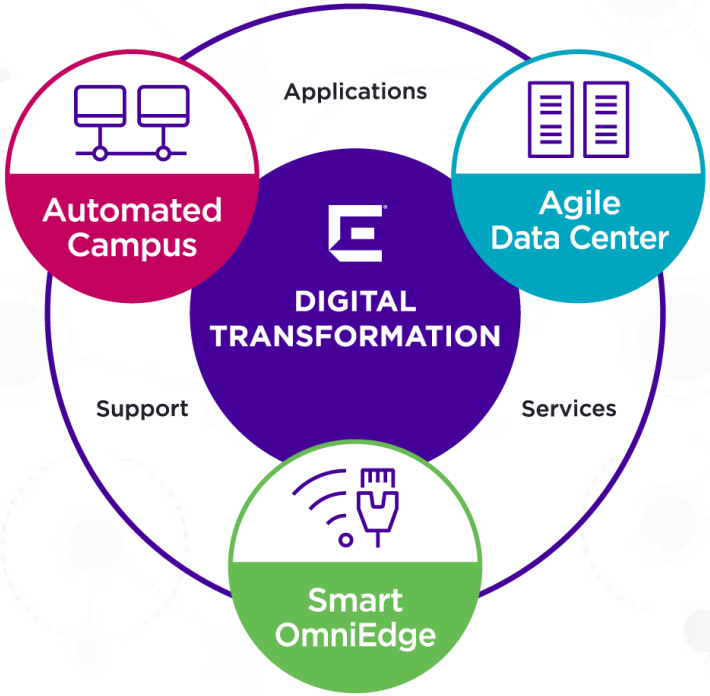
- Чай
- Кофе
- Пирожные

Часть 2: Демонстрация работы Extreme Automated Campus

- Конфигурирование фабрики «с нуля»
- Создание сервисов L2VSN, IP Multicast over L3VSN
- Работа механизма Fabric Attach

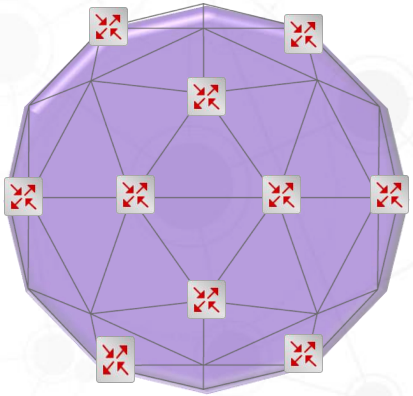
Что такое Extreme Automated Campus

Extreme Networks: Цифровая трансформация

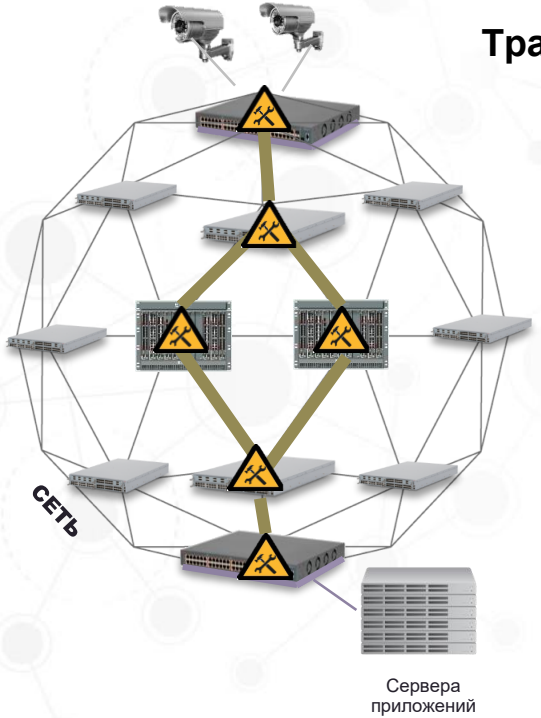


Что такое Extreme Automated Campus?

- Виртуализация всей сетевой инфраструктуры – «сетевое облако» для пользователей
- Основано на стандарте 802.1aq SPBm (ISIS + MacInMac)
- Предоставление всех корпоративных сервисов: L2, L3, IPVPN, IP Multicast при помощи одного протокола ISIS
- Сокращение времени и стоимости обслуживания сети
- Абсолютно любая физическая топология
- Встроенная безопасность

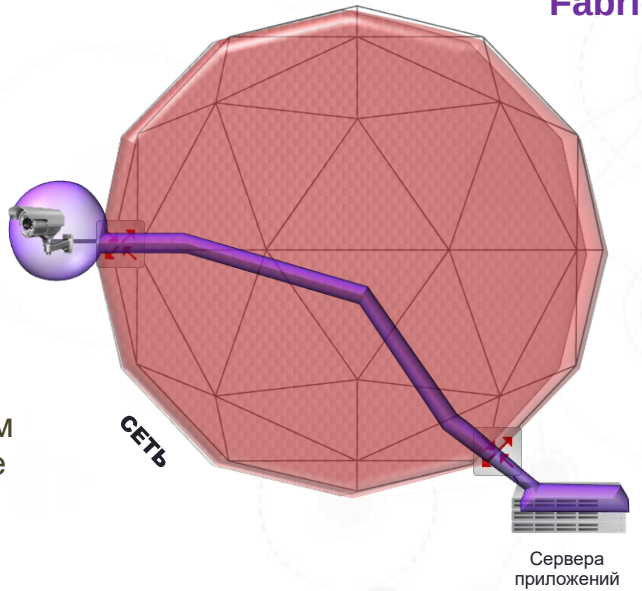


Скорость: включение сервиса на пограничных узлах



Традиционная сеть

- Поузловая настройка
- Добавление, удаление и перемещение - требует перенастройку сети
- Уязвима к ошибкам при перенастройке
- Услуги зависят от физической топологии



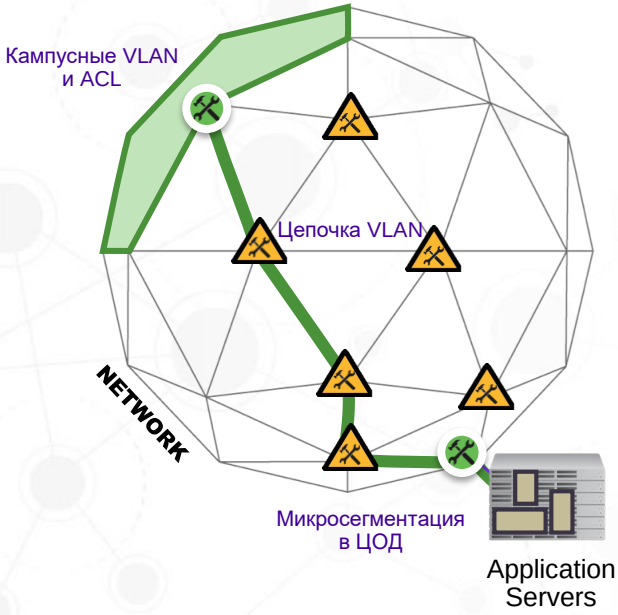
Fabric Connect

- Настраиваются только пограничные узлы
- Ядро не перенастраивается
- Добавление, удаление и перемещение делается без простоев
- Сервисы предоставляются независимо от топологии сети

Безопасность и гиперсегментация

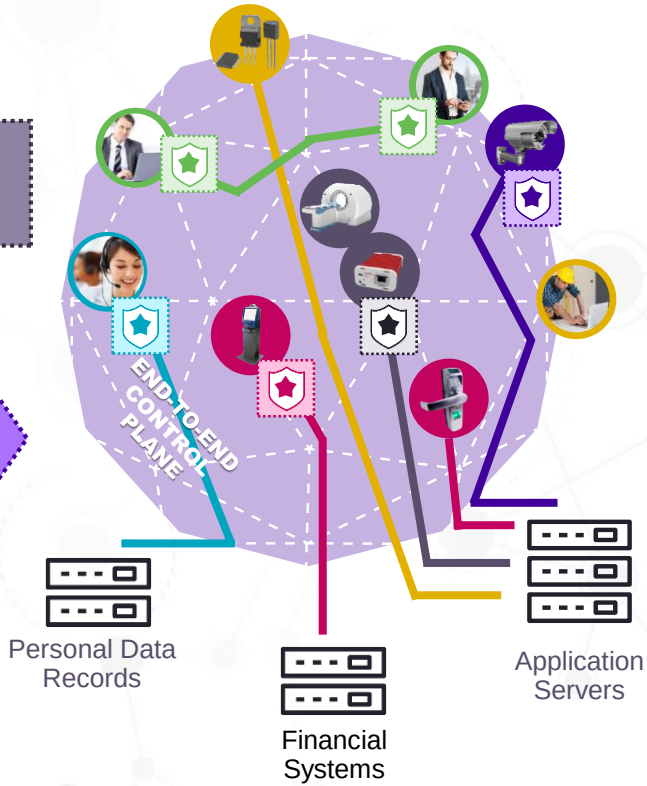
Предотвращение взлома сети

Automated Campus



Изоляция трафика частичная и не масштабируется

Сервисы с микросегментацией легко масштабируются

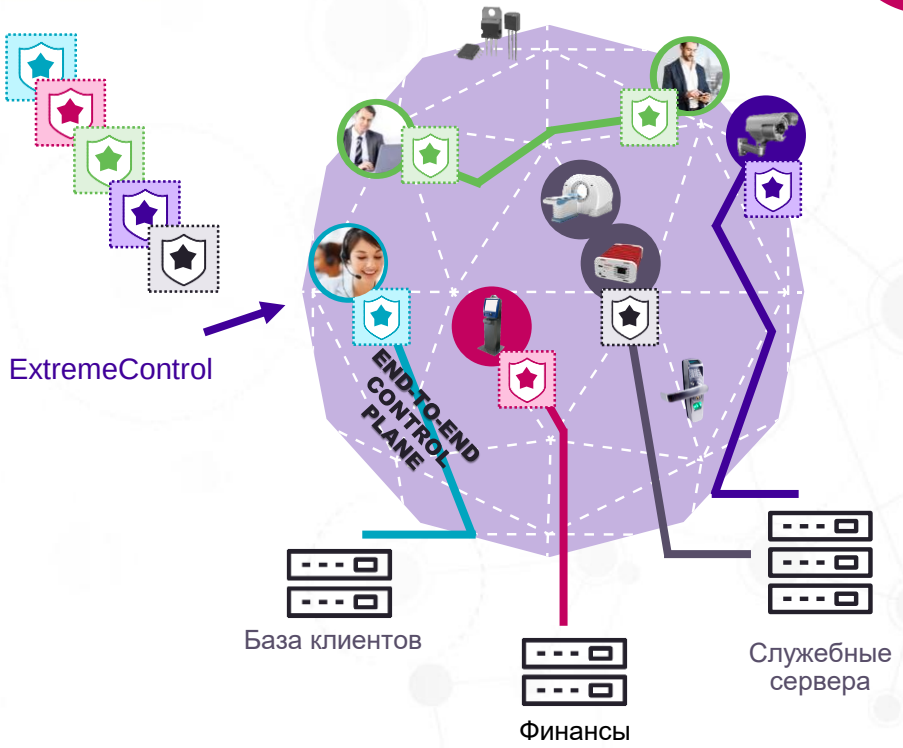


Автоматизированная безопасность

Подключение пользователей согласно политикам

Automated Campus

- Изоляция трафика end-to-end : гиперсегментация сети
  - Изолирование критичных приложений, устройств или пользователей
  - Нет возможности перейти от взломанной системы у другим системам
- Защита подключений при помощи политик Extreme Control
  - Кто или что может быть подключено к определенному сегменту
- Динамическая гиперсегментация и применение политик



Повышение безопасности БЕЗ усложнения системы

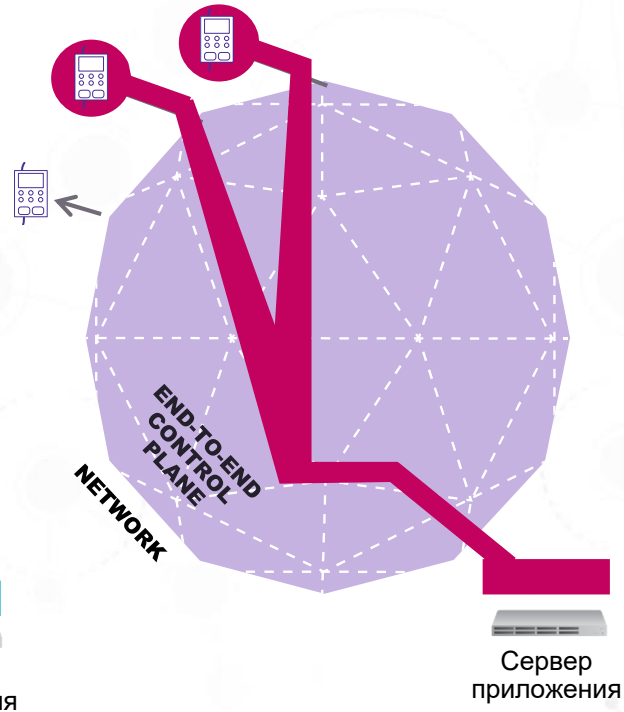
Эластичные сервисы безопасности

нет возможности организовать BackDoor

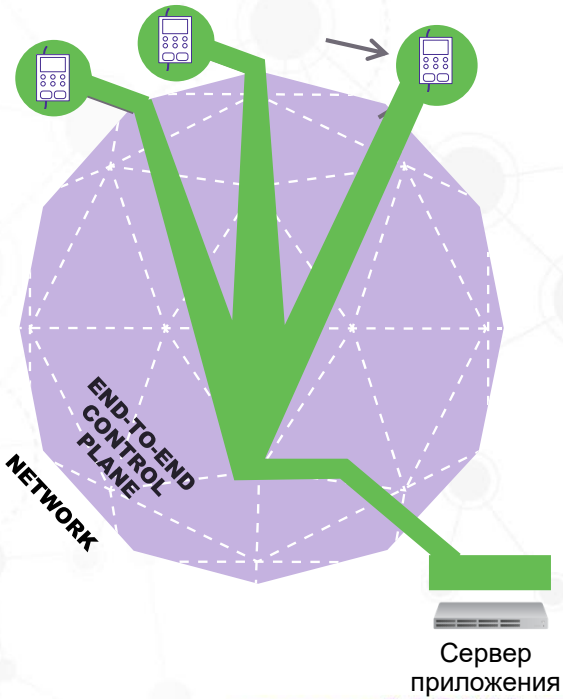
Automated Campus

Устройства IoTs в единой зоне безопасности

Устройство IoT отключено – сервис автоматически убран



Устройство IoT перемещено – зона соответственно изменяется



EXTREME NOW

Надежность Fabric Connect

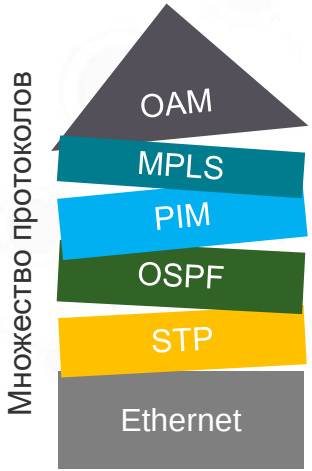
минимальное время восстановления сети

- Балансировка трафика active/active
- Полное восстановление сети за миллисекунды (L2/L3 и multicast)
- Нет «эффекта домино» наложенных протоколов
- Быстрое восстановление сети не влияет на уровень приложений

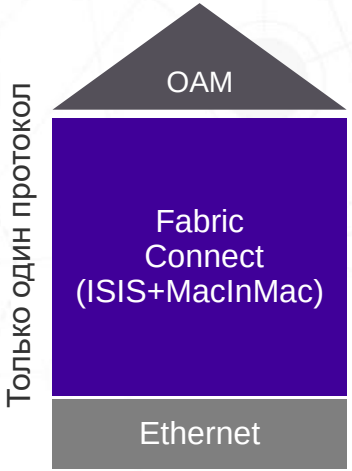
Fabric Connect – краткий обзор технологии

1. Базируется на стандарте 802.1aq Shortest Path Bridging с расширениями Extreme
2. Использует ISIS протокол как L2/L3 control plane
3. Для передачи трафика используется Mac-in-Mac инкапсуляция 802.1ah
4. Использует идентификацию и изоляцию сервисов I-SID (Independent Service Identifier)

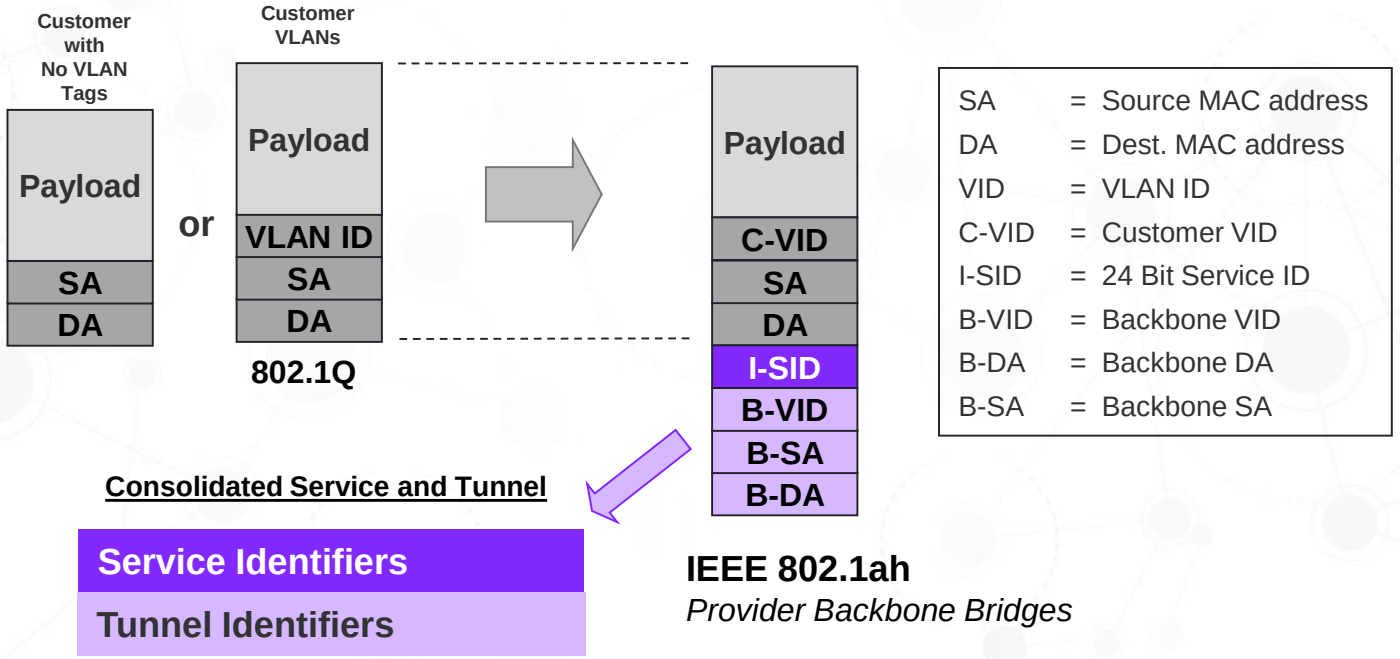
Традиционные сети:
Каждый протокол настраивается отдельно



Fabric Connect:
Простота настройки, выявления неисправностей



Инкапсуляция IEEE 802.1ah Mac-in-Mac



Простота коммутации без сложности с MPLS метками!

Базовые типы сервисов Fabric Connect

L2 VSN

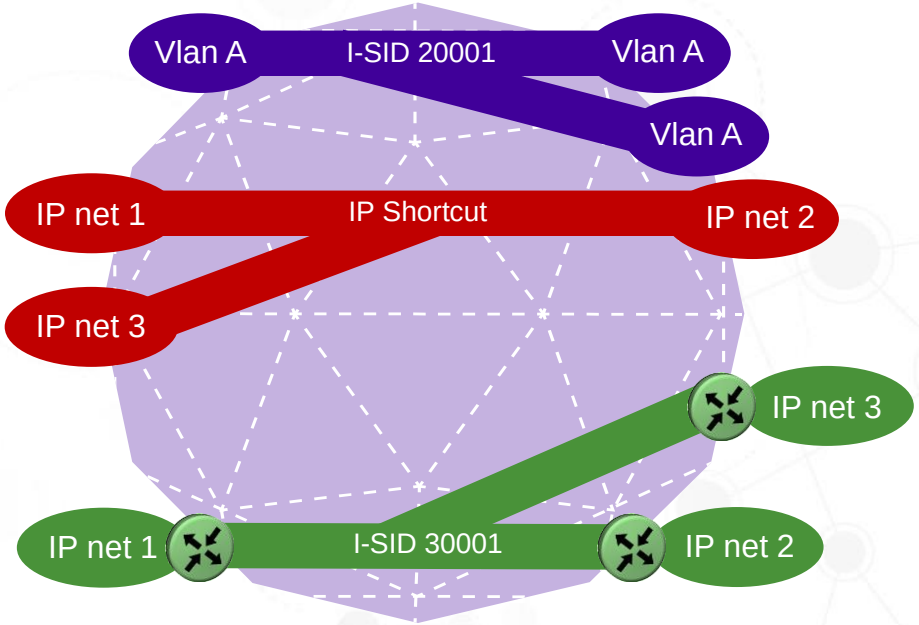
- Сервис L2 (VLAN)
- Поддержка Multicast IGMP

IP Shortcut

- GRT маршрутизация IPv4/IPv6
- IP Multicast routing

L3 VSN

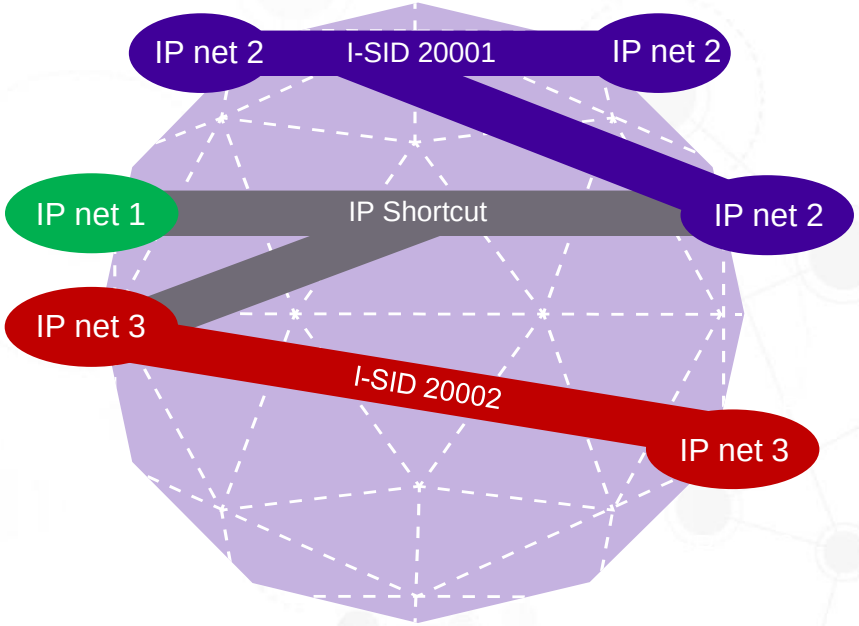
- Виртуализированная IPv4/IPv6 маршрутизация IPVPN
- Маршрутизация IP Multicast внутри IPVPN



Базовые типы сервисов Fabric Connect: соединение сервисов

IP Shortcut и L2VSN

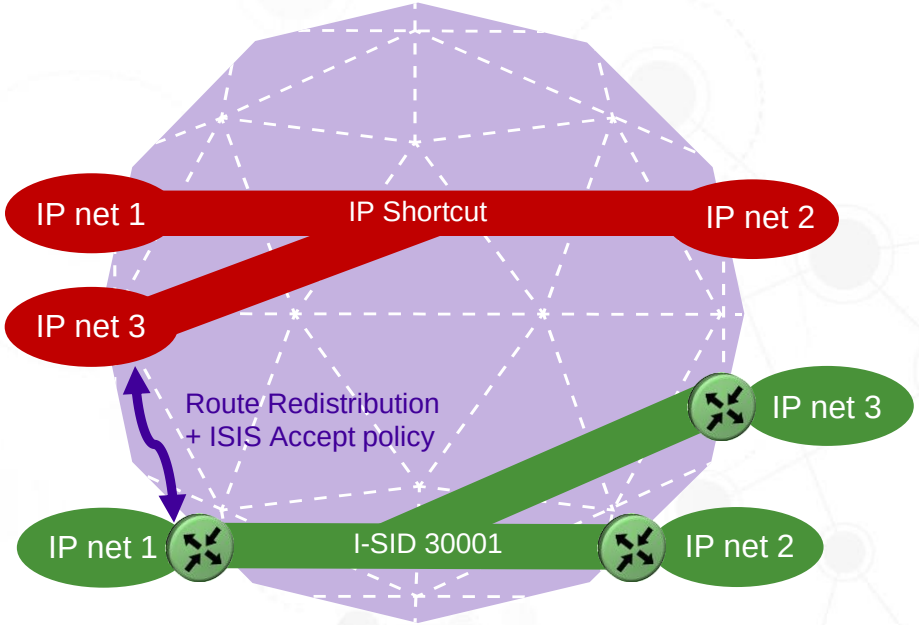
- Нужный влан в любой точке сети
- Абсолютная гибкость



Базовые типы сервисов Fabric Connect: Inter-VRF Route Leaking

Inter-VRF Routing

- Обмен части маршрутной информации между разными IPVPN/GRT
- Выбор нужных маршрутов при помощи ISIS Accept Policy

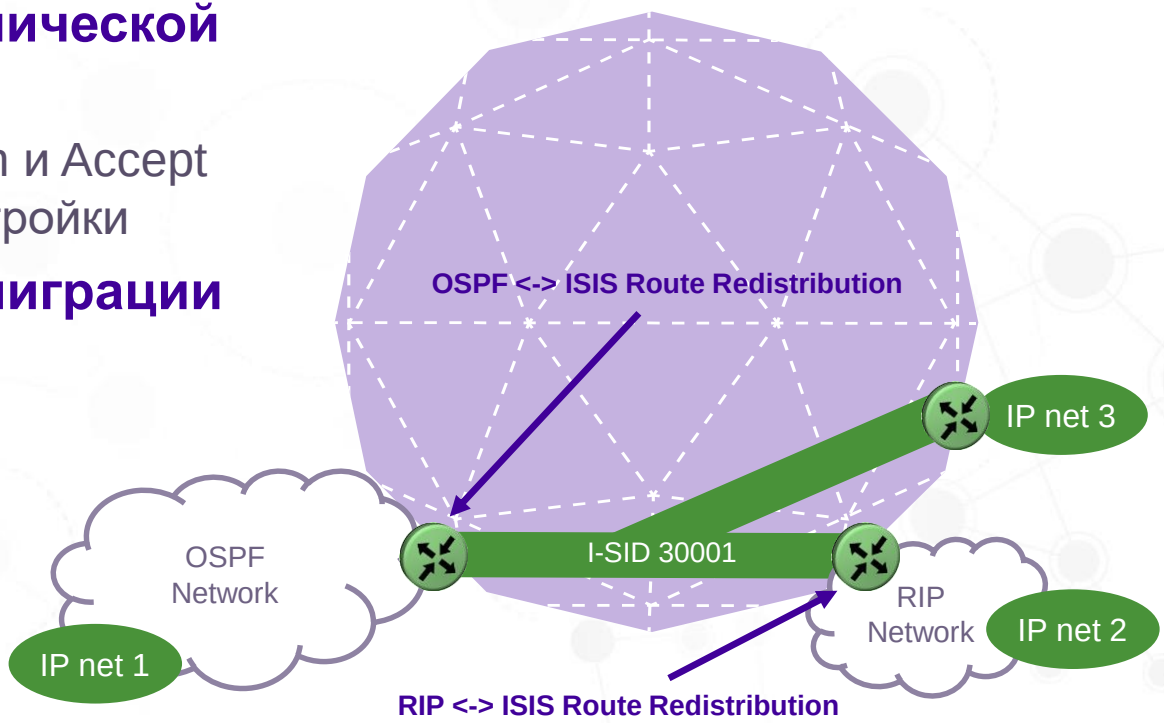


Интеграция Fabric Connect с RIP/OSPF/BGP

ISIS как протокол динамической маршрутизации

- Политики Redistibution и Accept policy для тонкой настройки

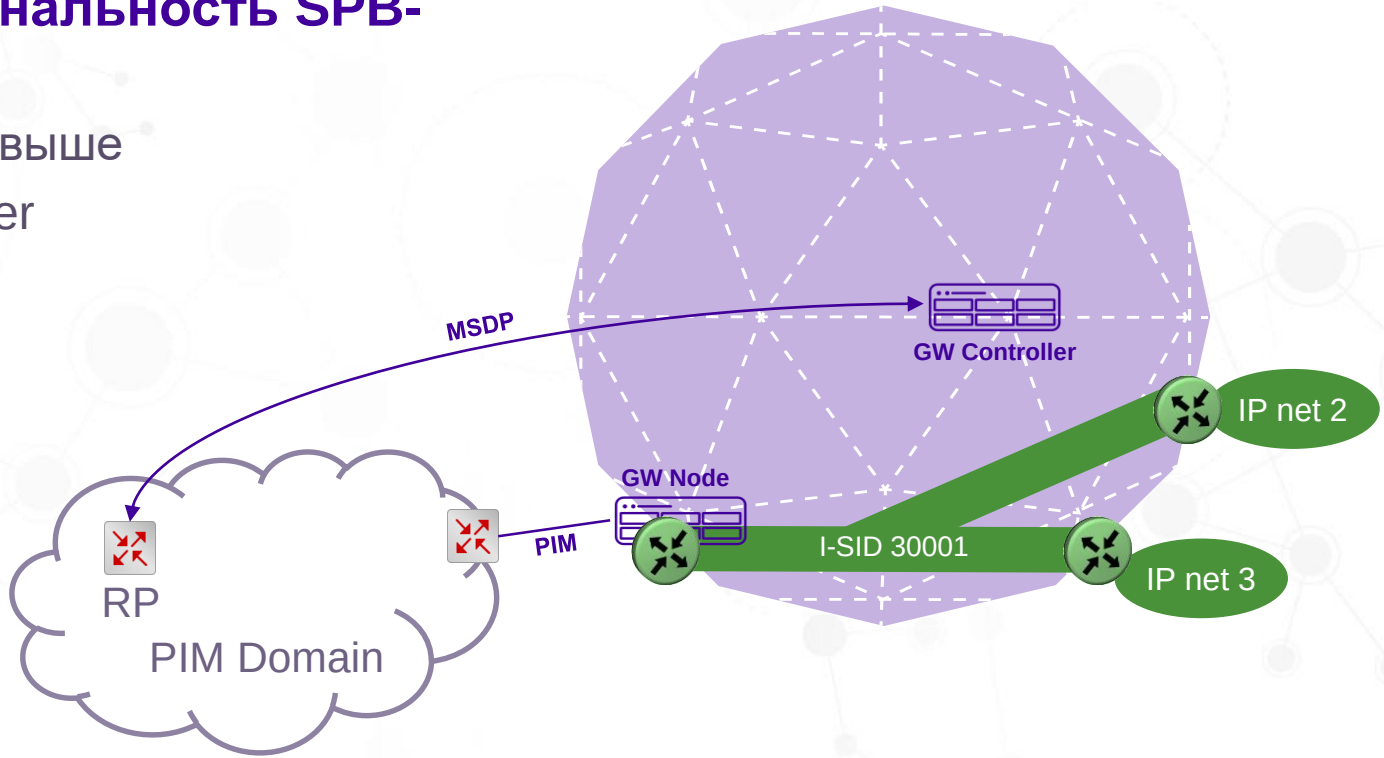
Решение для плавной миграции на Fabric Connect



Интеграция Fabric Connect с доменами PIM

Новая функциональность SPB-PIM GW

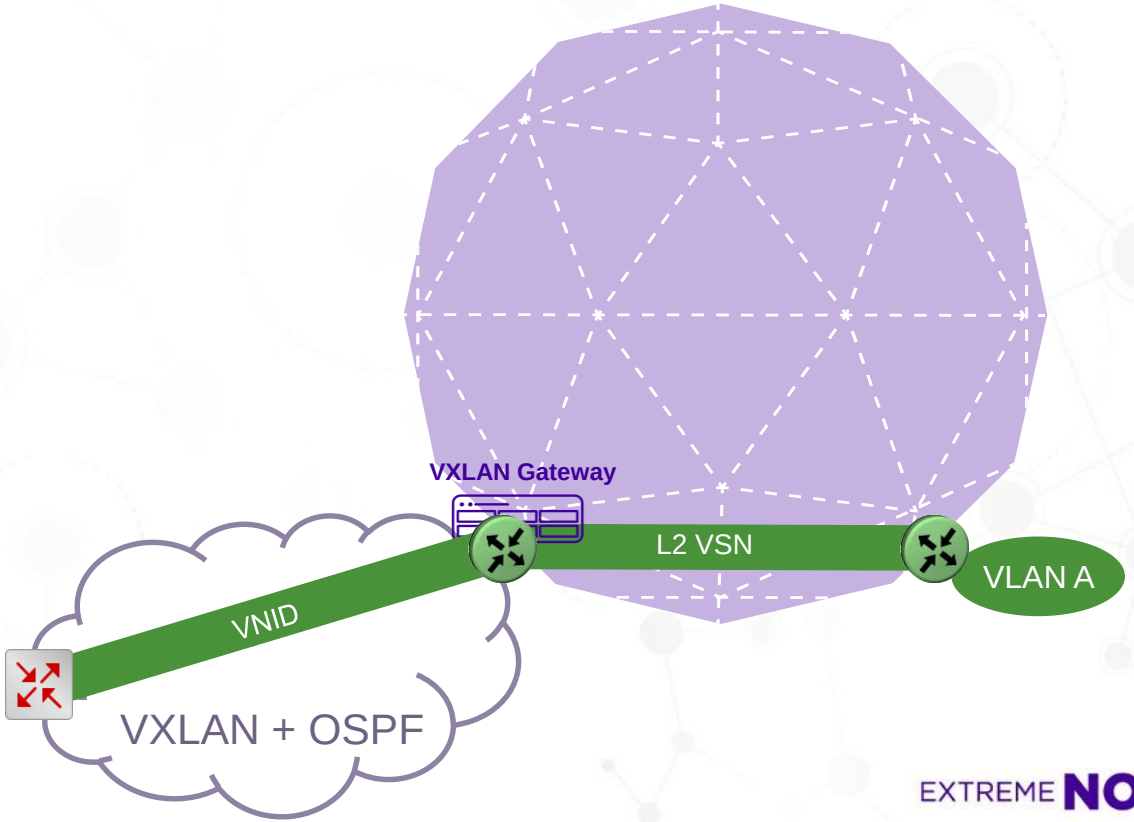
- VOSS 6.0 и выше
- GW Controller
- GW Nodes



Интеграция Fabric Connect с VXLAN

VXLAN Gateway

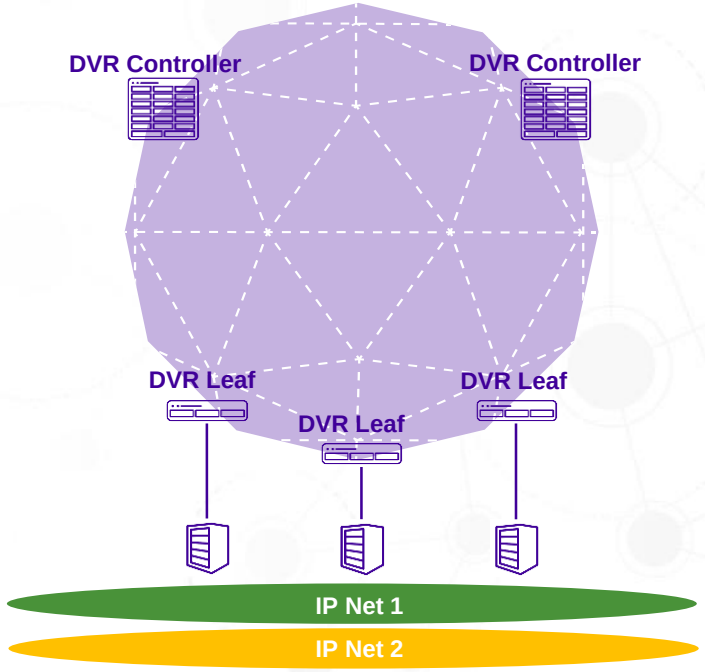
- VOSS 6.0 и выше
- VXLAN-to-VLAN L2
- VXLAN-to-VXLAN L3
- VXLAN-to-SPBm
- Поддержка OVSDB
- Premier License



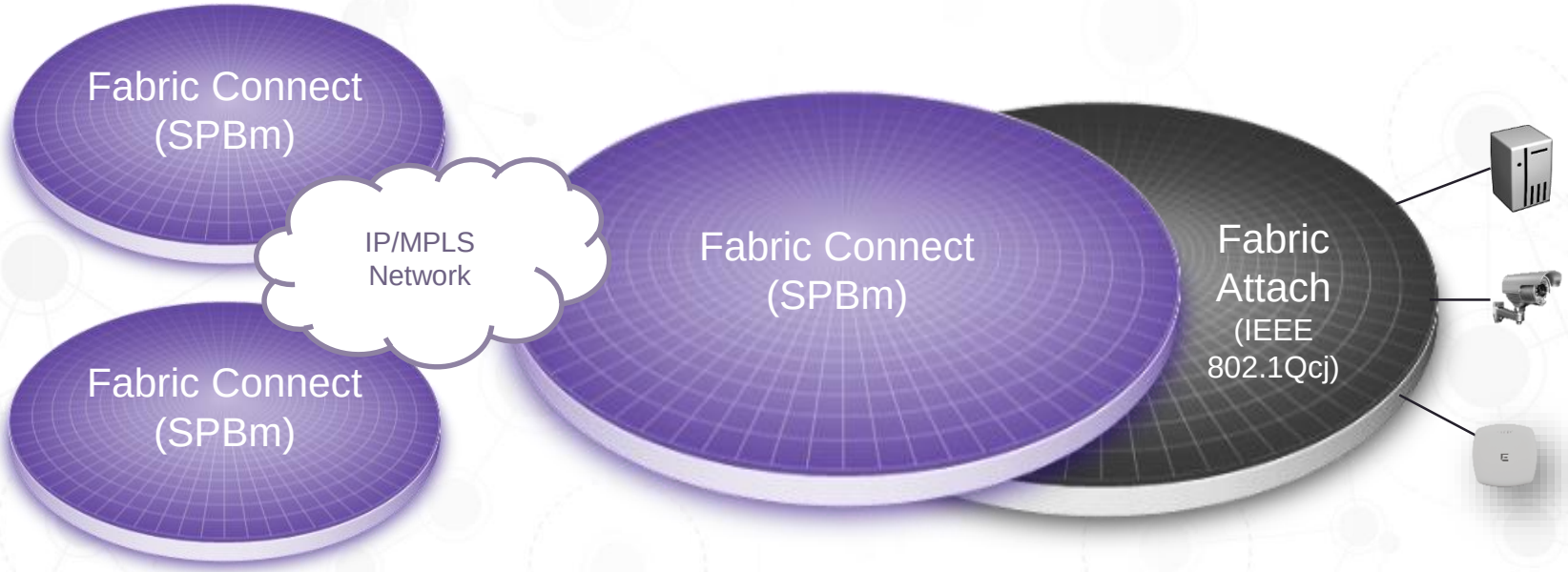
Распределенная маршрутизация DVR

Distributed Virtual Routing

- VOSS 6.0 и выше
- Оптимизация миграции VM в ЦОД
- Маршрутизация между подсетями на уровне Leaf
- Premier License только на контроллере



Экосистема Automated Campus: не только Fabric Connect



Fabric Extend – возможность расширения фабрики на удаленные площадки/узлы поверх IP инфрастуктуры

Fabric Connect – основа для ядра, распределения и доступа

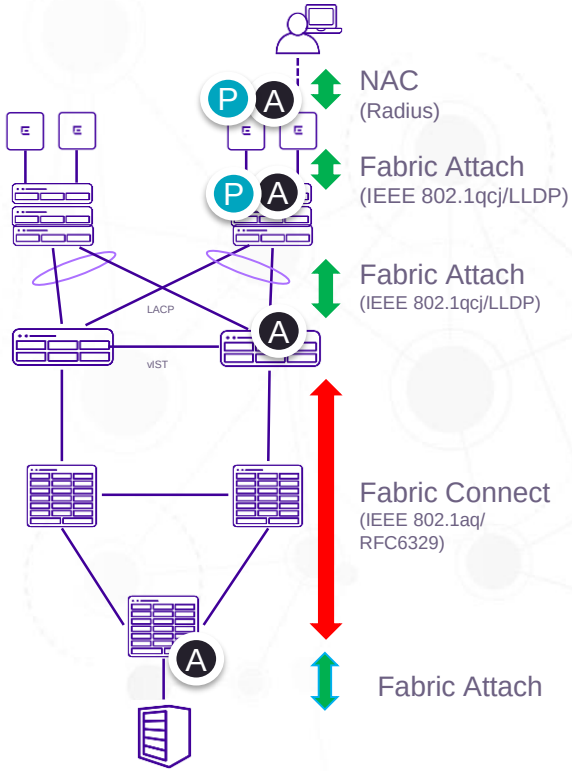
- Быстрая
- Гибкая
- Безопасная

Fabric Attach – автоматическое и безопасное подключение к сервисам фабрики не-SPBm оборудования

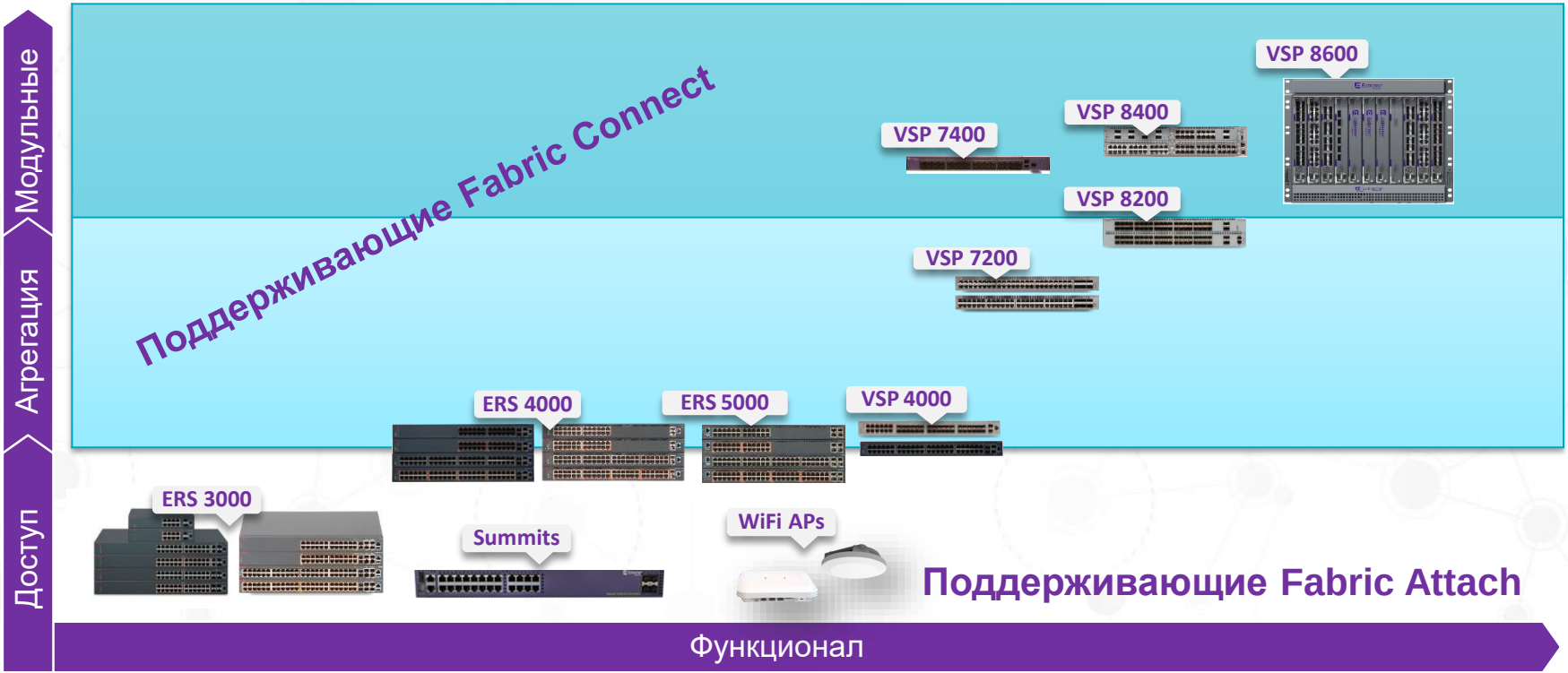
Fabric Attach: автоматизация уровня доступа

Подключение пользователя

- Проверка политик авторизации пользователя на NAC
- Применение политик на свиче или точке доступа (P)
- Динамическая сигнализация VLAN-ISID до уровня Fabric Connect
- Аналитика трафика на свичах и точках доступа (A)



Портфолио Fabric Networking в деталях



Вопросы и перерыв

Демонстрация Extreme Automated Campus

Схема тестового стенда

Fabric Connect

– VSP 8400-1,
VSP 8400-2,
ERS 5900

Fabric Attach

– X440-G2

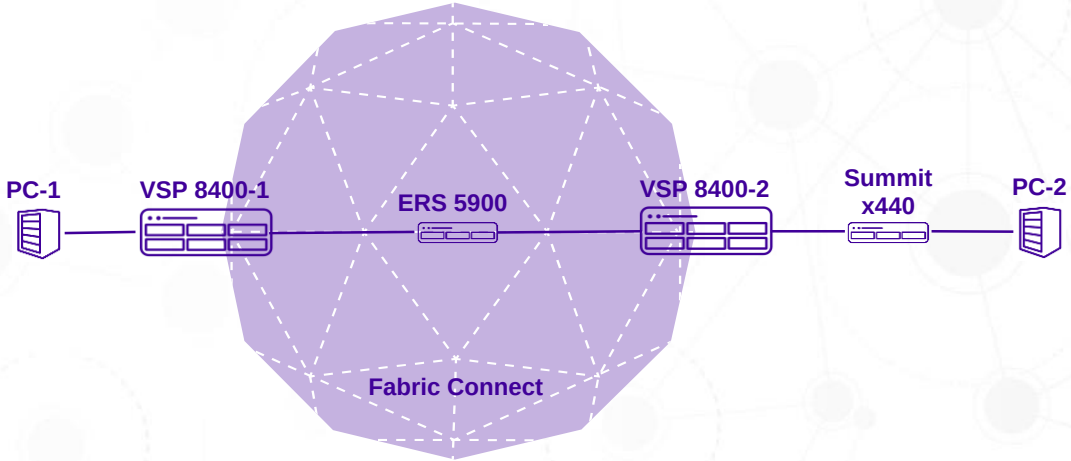


Схема тестового стенда

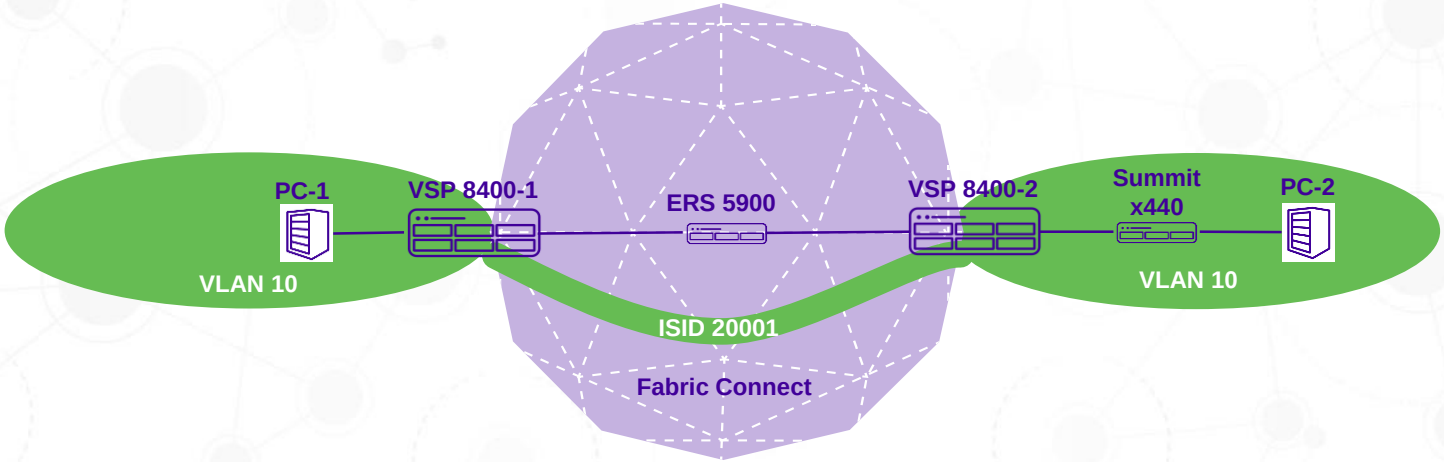
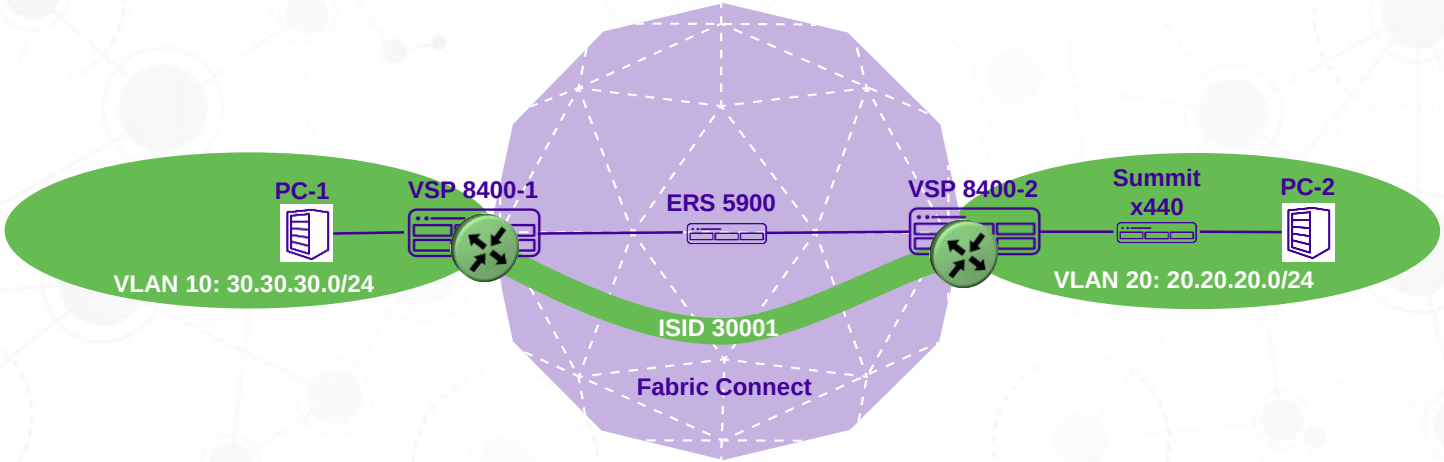


Схема тестового стенда




EXTREME
NOW
WORLD TOUR