

Архитектура корпоративной сети Cisco, варианты внедрения и позиционирование

Илья Озарнов
Системный инженер
iozarnov@cisco.com

Программа

Задачи презентации

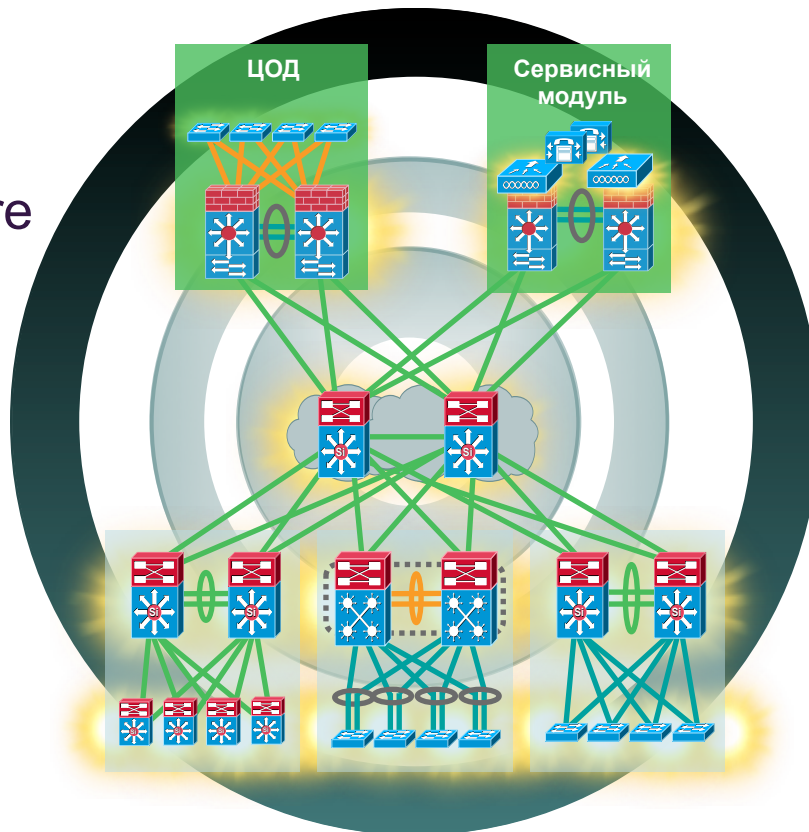
Обзор ключевых сервисов

Reference Network Architecture

Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- Converged Access
- Instant Access

Заключение



Задачи презентации

По результатам этой презентации слушатели должны:

Понять характеристики различных моделей дизайна корпоративных сетей

- Unified Access
 - Традиционный доступ
 - Converged Access
 - Instant Access

Понять какие платформы являются ведущими для различных моделей дизайна

- Позиционирование продуктов

Принимать решения о выборе модели дизайна и продуктов в соответствии с требованиями проекта

- Понимание текущих требований и преимуществ, которые может обеспечить та или иная модель дизайна
- Понимание ключевых критериев для выбора модели дизайна корпоративной сети

Модели дизайна корпоративной сети

Традиционный доступ, конвергированный доступ и Instant Access

Унифицированный доступ

Единое управление



Cisco Prime Infrastructure

Cisco ISE

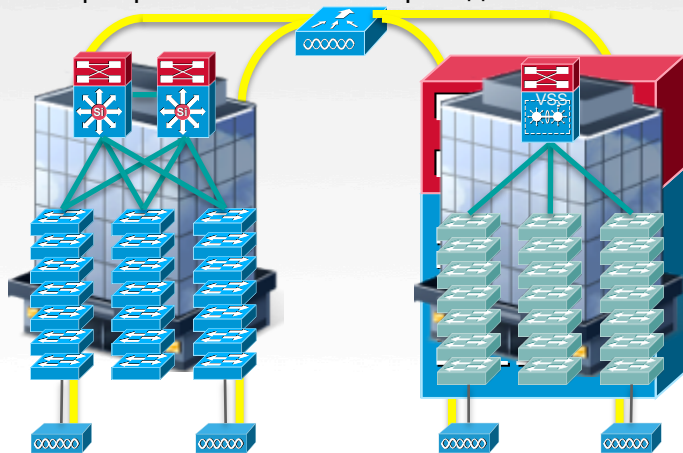


Единая политика

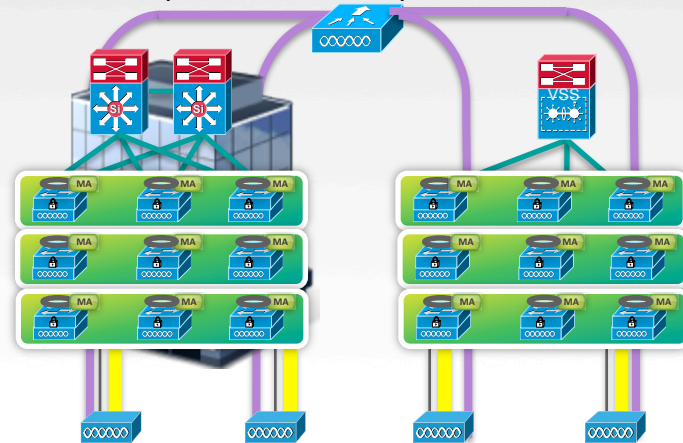
Централизованная беспроводная сеть

Распределённая беспроводная сеть

Распределённая проводная сеть



Централизованная проводная сеть



Распределённая проводная сеть

Традиционный
Доступ

Instant Access

Конвергированный доступ

Unified Access

Что это на самом деле означает?



Cisco Prime
Infrastructure



Identity
Services Engine

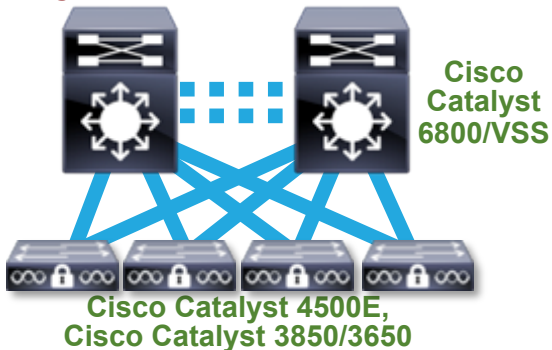
Ведущие платформы



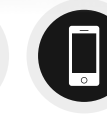
WISM2/
WLC



WLC



Wireless
точки
доступа



КЛЮЧЕВЫЕ СЕРВИСЫ ВНЕДРЕНИЙ UNIFIED ACCESS

Безопасность TrustSec

Secure Group Access для упрощения сети и использования виртуализации

Application Visibility and Control

Application-Aware Networking для сервисов Collaboration, Video и других приложений

Надёжность и гибкость

Высокая надёжность сети с использованием Virtual Switching и Stateful SwitchOver

Smart Operations

Снижение операционных расходов и оптимизация обеспечения работы сервисов

Программа

Задачи презентации

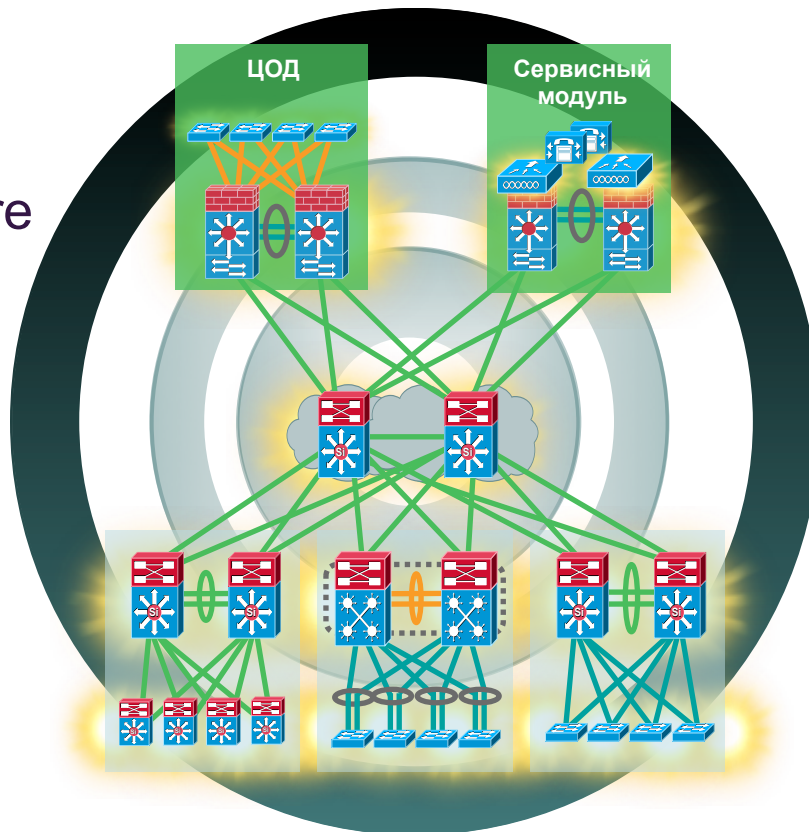
Обзор ключевых сервисов

Reference Network Architecture

Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- Converged Access
- Instant Access

Заключение



Сеть в качестве инструмента безопасности

Сеть как сенсор



Больше информации
Богаче контекст

Сбор информации об угрозах
Быстрое обнаружение

ISE + NetFlow + Lancopre

Сеть как регулятор



Программно-определяемая
сегментация

Уменьшение возможностей
для атаки

ISE + TrustSec

Visibility with Flexible NetFlow

Fits all the needs for high-flow backbone environments

Can I Identify and Prioritize Critical Data traffic?

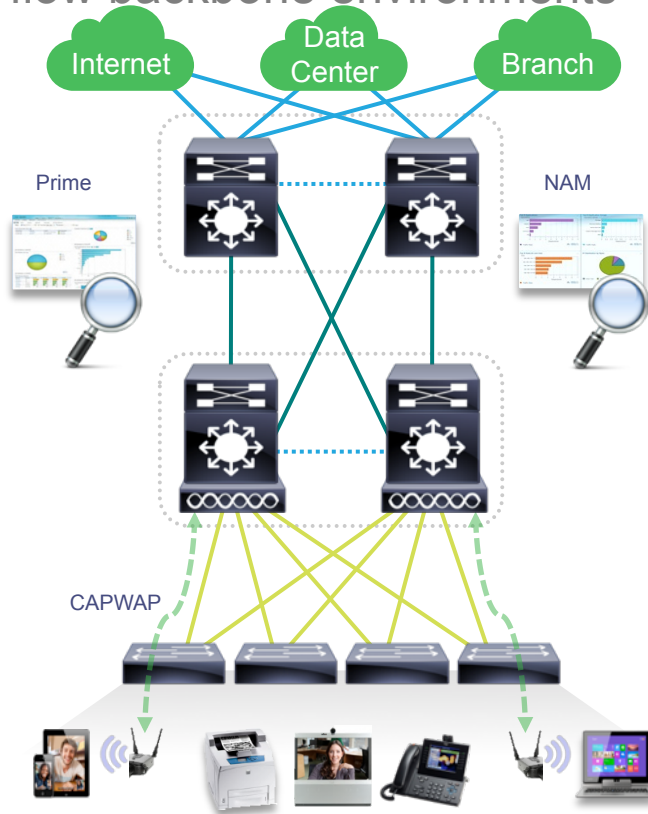
Can I monitor hosted workloads?

Can I Debug issues such as video and voice quality?

Can I quickly isolate and troubleshoot latency issues?

Are there any packet and protocol level anomalies?

Is there an anomalous traffic pattern?



Flexible NetFlow

Account for L2 switched/bridged IPv6 traffic

Sampled NetFlow in Hardware

Optimize the NetFlow tables utilization and minimize load on analyzers

Multicast Visibility with Egress NetFlow

Single point of configuration for full visibility

Bigger Tables

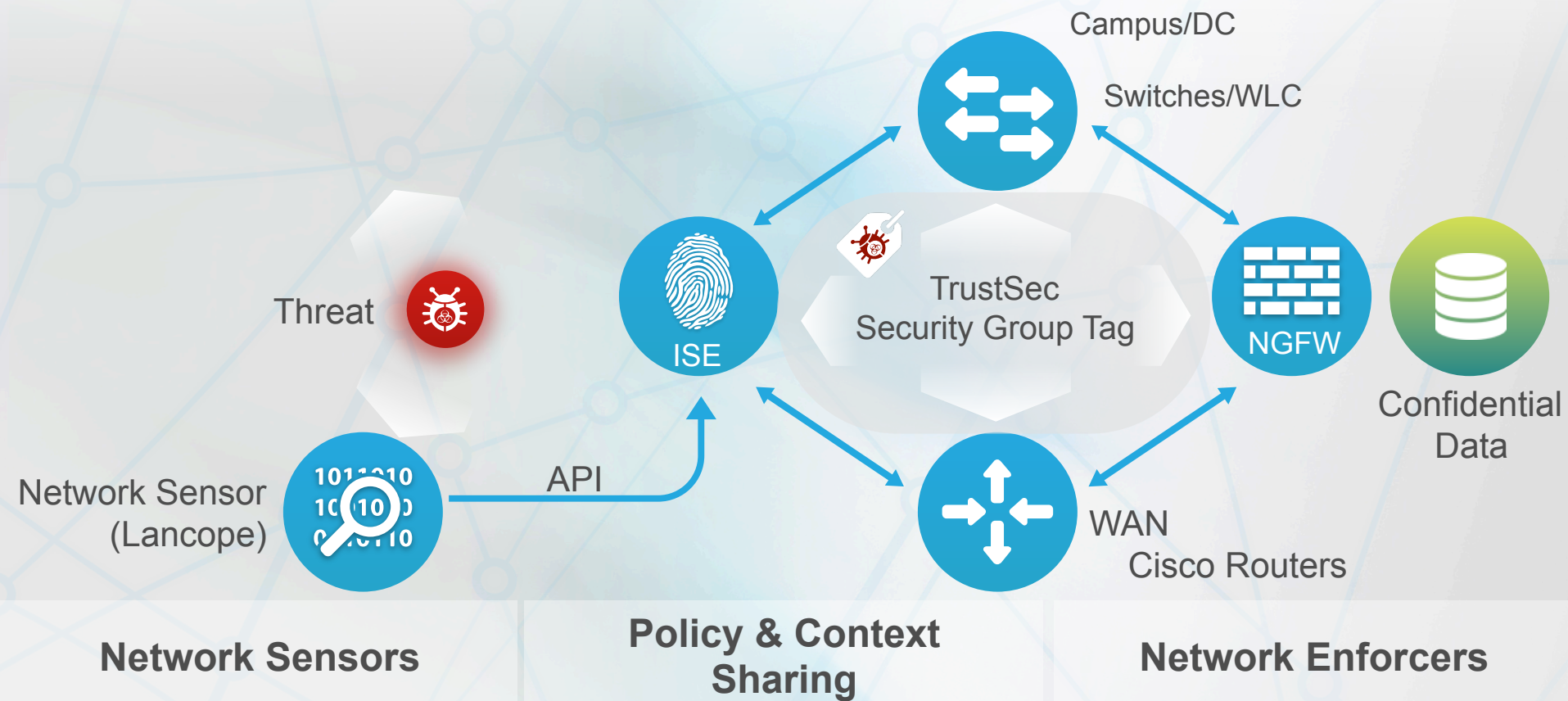
For more entries per DFC, up to 13m flows

Optimal CPU utilization

With yielding NetFlow data export, direct export from line card

Architecting Security


Uniting Embedded & Dedicated Securities for Threats



Технология Cisco Trustsec

Сегментация на основе бизнес-политик




Политика
сегментации

Source Zone

Destination Zone

		Hospital Zone				DC Zone			
		PCI Device	Clinical Device	Staff	Guest	Core Service Servers	Update Service	PCI Database	EHR DB
Hospital Zone	PCI Device	✓	X	X	X	✓	✓	✓	X
	Clinical Device	X	✓	X	X	✓	✓	X	✓
	Staff	X	X	X	X	✓	✓	X	X
	Guest	X	X	X	✓	X	X	X	X

Традиционная политика безопасности

Автоматизация управления системой безопасности

Повышение эффективности

Упрощенное управление доступом



Коммутатор



Маршрутизатор



Межсетевой
экран ЦОД

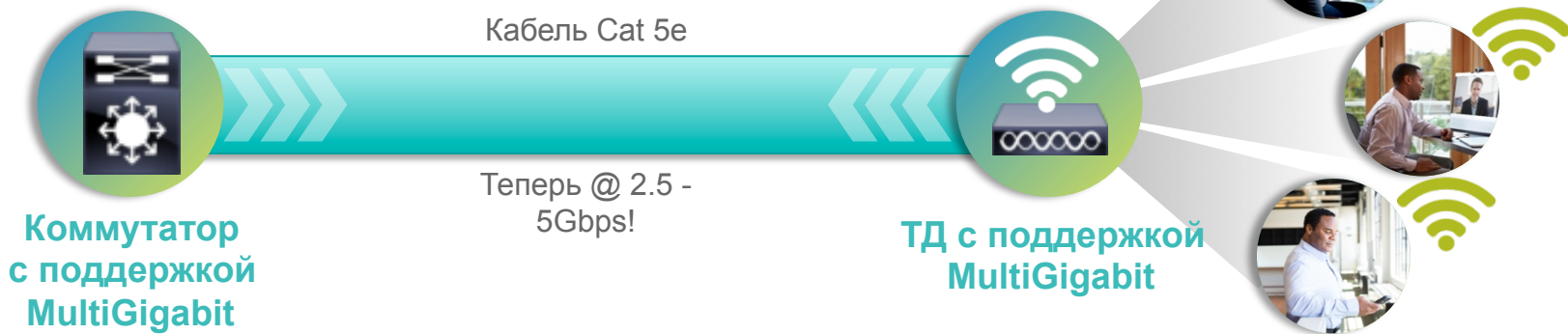


Коммутатор ЦОД

Гибкое и масштабируемое применение политик

Увеличение пропускной способности на уровне доступа

MultiGigabit NBASE-T



Cisco MultiGigabit с **NBASE-T**™

Инновация, позволяющая масштабировать уровень доступа за 1 Гбит/с

Возможность использования 2.5 и 5 Gbps на расстояниях до 100 м по существующей СКС

Поддержка всех стандартов PoE вплоть до 60 Вт

Увеличение пропускной способности до 5 раз без необходимости модернизации существующей СКС

Увеличение пропускной способности на уровне распределения/ядра

40 Гбит/с?

Клиенты с высокими требованиями к полосе

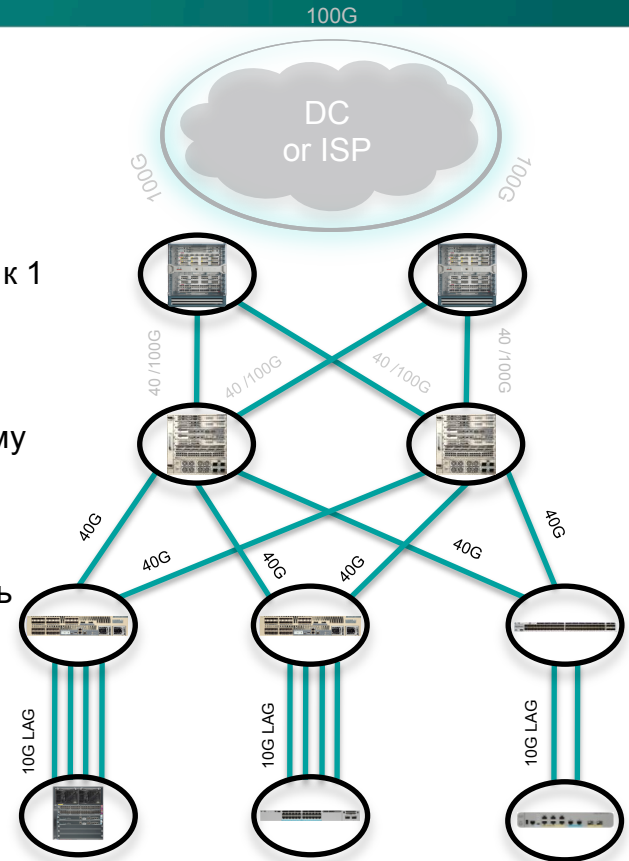
- Увеличение плотности клиентов с высокими требованиями к полосе (802.11ac Wave 2)
- Увеличение вероятности появления индивидуальных потоков близких к 1 Гбит
- Повсеместное распространение ВКС и увеличение видео трафика

Оптимизация полосы

- Агрегация каналов и балансировка могут приводить к субоптимальному использованию
- Агрегация 1G или 10G LAG дает меньше, чем $N \times 1$ или 10G реально используемой полосы
- Максимально агрегируется 8 портов, что дает 8G или 80G макс на путь

Простота управления

- Меньше портов и трансиверов, которые необходимо покупать и обслуживать
- Меньше конфигурация
- Проще и надежнее внедрение таких функций, как QoS



Application Visibility and Control (AVC)

Внедрения BYOD и угрозы для ваших приложений

Проблемы IT

- Готова ли сеть для внедрения видео?
- Как обеспечить качественную работу бизнес-приложений?
- Как обеспечить эффективный мониторинг и поиск неисправностей?



Анализ и сбор информации

- Enhanced Object Tracking
- IP SLA
- Built-in Traffic Simulator
- Cisco CleanAir

Идентификация и контроль приложений

- Media Services Proxy (MSP)
- Metadata
- Flexible NetFlow
- Device sensor
- Secure group tagging
- Quality of Service (QoS)
- AVC in Wireless Controller

Мониторинг и устранение неисправностей

- Performance Monitor
- Mediatrace
- Flexible NetFlow
- Wireshark / Mini-Protocol Analyzer
- Device sensor

High Availability → L2/L3

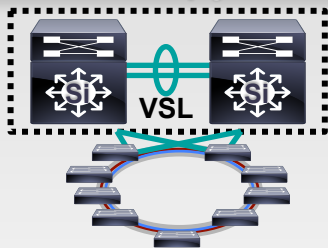
Multicast: HA, Call Admission Control (CAC), Multipath, Video Stream

Гибкость инфраструктуры – доступ

Cisco StackWise+



Масштабируемость



- Расширение сетевого доступа в рамках одного логического устройства
- Высокопроизводительное двунаправленное кольцо в стеке
- Одна логическая единица для управления 9 коммутаторами, 450 портами

Упрощение управления



- Архитектура с централизованным контролем и управлением
- Уменьшение кол-ва VLAN'ов/ подсетей
- 9-ти кратное упрощение эксплуатации

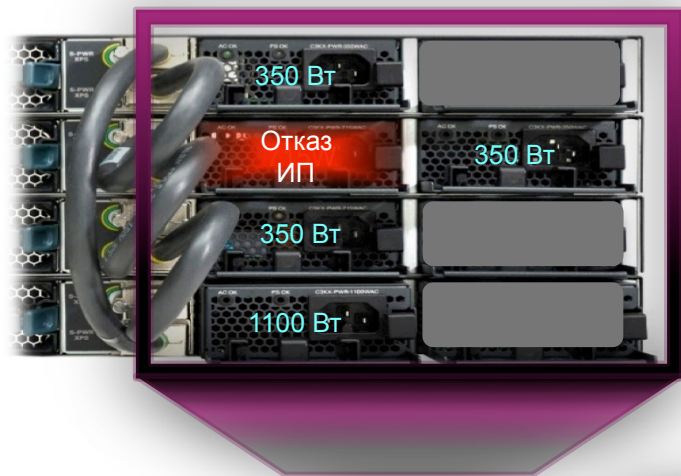
Гибкость



- Гибкая и распределенная архитектура коммутации
- Единая сеть
- Эксплуатация сети без прерывания сервисов коммутации

Гибкость инфраструктуры - доступ

Cisco StackPower обеспечивает резервирование питания



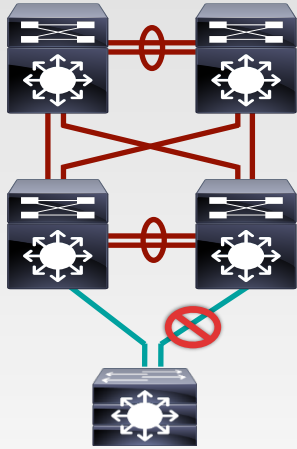
- Все источники питания в стеке формируют **общий бюджет по питанию** независимо от мощности, типа AC/DC и местоположения
- Режим резервирования обеспечивает **1+n защиту** от отказа наиболее мощного ИП в стеке, выделяя его мощность в специальный резервный бюджет
- Оставшийся бюджет распределяется между потребителями питания: коммутаторами и PoE-устройствами
- В случае отказа линии питания, выхода из строя или замены ИП, недостаток мощности компенсируется из резервного бюджета, обеспечивая **непрерывность бизнес-процессов и коммуникаций**

Более детальная информация: [Calculating Power for Cisco StackPower](#)

Гибкость инфраструктуры – ядро/распределение

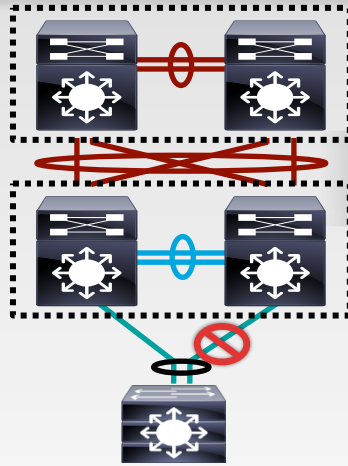
Virtual Switching System (VSS)

Традиционный дизайн



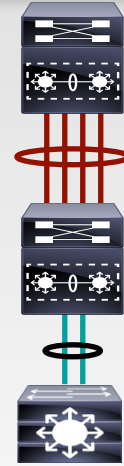
Оптимизация
сети

VSS-дизайн



Упрощение
эксплуатации

VSS-дизайн



- Комплексный сетевой дизайн и эксплуатация
- Неполное использование сетевых ресурсов
- Неоптимальная производительность приложений и сети

- Оптимизированный сетевой дизайн
- Удвоение пропускной способности коммутации
- Оптимизированная производительность приложений и сети

- Упрощенная эксплуатация системы
- Единое логическое сетевое устройство
- Упрощенная и отказоустойчивая сетевая топология

Гибкость инфраструктуры – обновление ПО

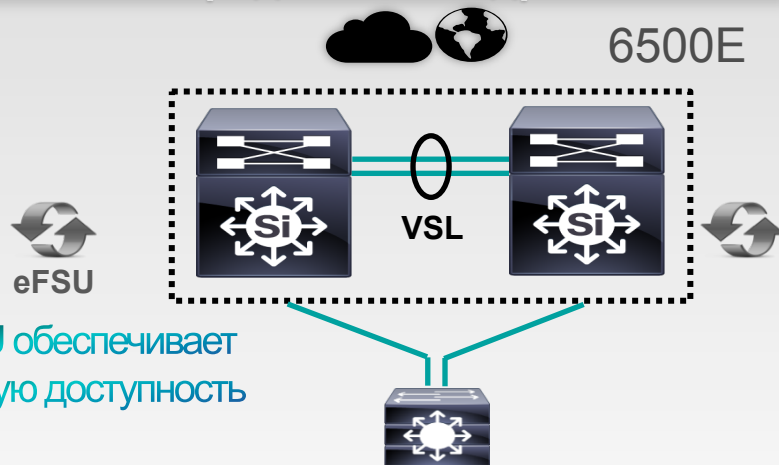
ISSU обеспечивает сетевую доступность 99,999%

Доступ



- Dual-Supervisor требует совместимости версий ПО
- ISSU обеспечивает апгрейд ПО в рамках одного шасси в режиме реального времени
- Защита сетевых сервисов и ресурсов, доступность для проводных и беспроводных конечных устройств

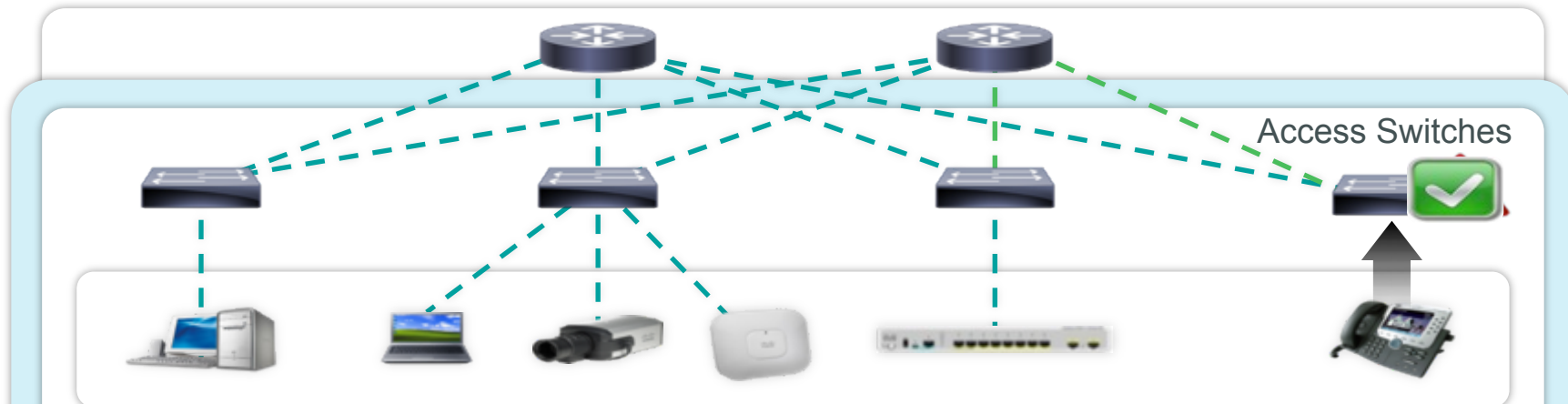
Распределение / ядро



- eFSU обеспечивает апгрейд ПО для двух шасси в режиме реального времени
- Защита сетевых сервисов и доступность с резервированием маршрутов на уровне доступа
- Влияние на сеть ~1 сек для всего процесса апгрейда

Cisco Smart Operations

Упростите свою инфраструктуру



PnP APIC EM

Подключен новый коммутатор

- Software image загружен; конфигурация автоматически применена
- **Zero Touch** внедрения, апгрейды и замены

Interface templates + AutoConf

Подключено новое устройство

- Настройки порта: Applied
- Политики QoS: Enforced
- Политики безопасности: Enforced

Упрощение задач управления

Embedded Event Manager

Автоматическая реакция на события

Кастомизация поведения IOS

- Изменение поведения IOS
- **Автоматическое** решение сетевых проблем
- **Автоматизация** реакции на происходящие события

Interface Templates

ДО

```
6500# show running-config interface GigabitEthernet 101/1/0/1
```

```
!  
interface GigabitEthernet 101/1/0/1  
switchport mode access  
switchport block unicast  
switchport port-security  
priority-queue out  
mls qos trust dscp  
spanning-tree portfast  
spanning-tree bpduguard enable  
end
```

```
6500# show running-config interface GigabitEthernet 101/1/0/2
```

```
!  
interface GigabitEthernet 101/1/0/2  
switchport mode access  
switchport block unicast  
switchport port-security  
priority-queue out  
mls qos trust dscp  
spanning-tree portfast  
spanning-tree bpduguard enable  
end
```



ПОСЛЕ

```
6500# show run template IA_INTERFACE_TEMPLATE
```

```
!  
template IA_INTERFACE_TEMPLATE  
switchport mode access  
switchport block unicast  
switchport port-security  
priority-queue out  
mls qos trust dscp  
spanning-tree portfast  
spanning-tree bpduguard enable  
end
```

```
6500# show run interface GigabitEthernet 101/1/0/1
```

```
!  
interface GigabitEthernet 101/1/0/1  
source template IA_INTERFACE_TEMPLATE  
end
```

```
6500# show run interface GigabitEthernet 101/1/0/2
```

```
!  
interface GigabitEthernet 101/1/0/2  
source template IA_INTERFACE_TEMPLATE  
end
```

Проще конфигурация, внесение изменений и поиск неисправностей

Программа

Задачи презентации

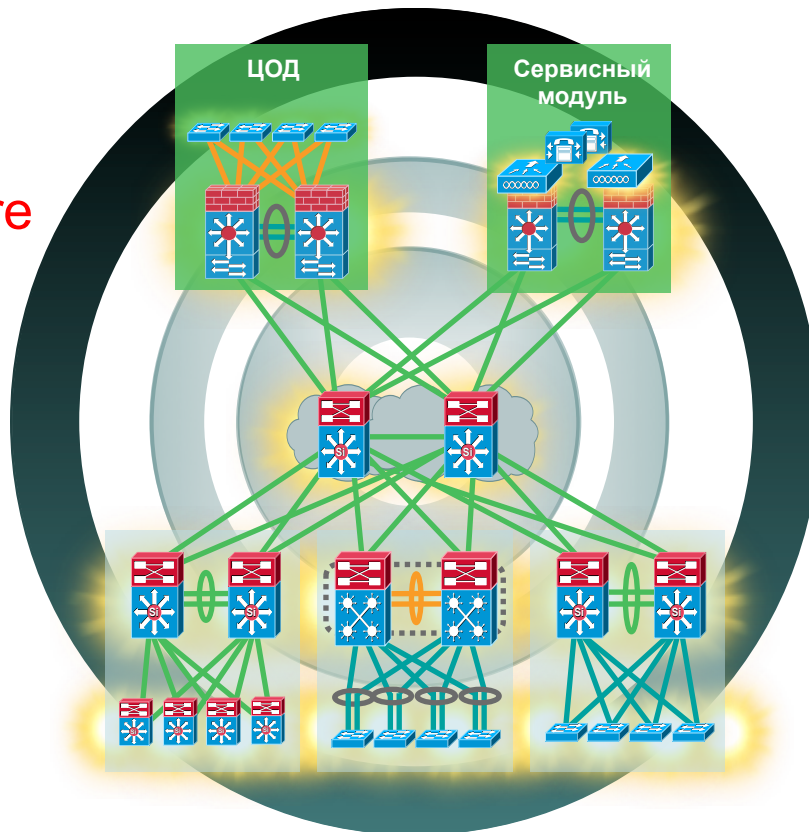
Обзор ключевых сервисов

Reference Network Architecture

Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- Converged Access
- Instant Access

Заключение



Задача

Мне нужно разработать дизайн сети...

Как предусмотреть возможность внедрения новых сервисов в будущем без необходимости внесения кардинальных изменений?

Как сделать это быстро?

Как управлять?

Как заставить сеть работать как единое целое?



Какую платформу выбрать?
Подбор платформы в зависимости от планируемой роли в сети

Catalyst 2960-X
Catalyst 3750X
Catalyst 3850
Cisco3945E
Catalyst 4500E
Catalyst 6807-XL
Catalyst 4500-X
Catalyst 6500
Catalyst 3650
ASR1000

Каковы best practices?



Cisco Design Zone

Рекомендации по дизайну

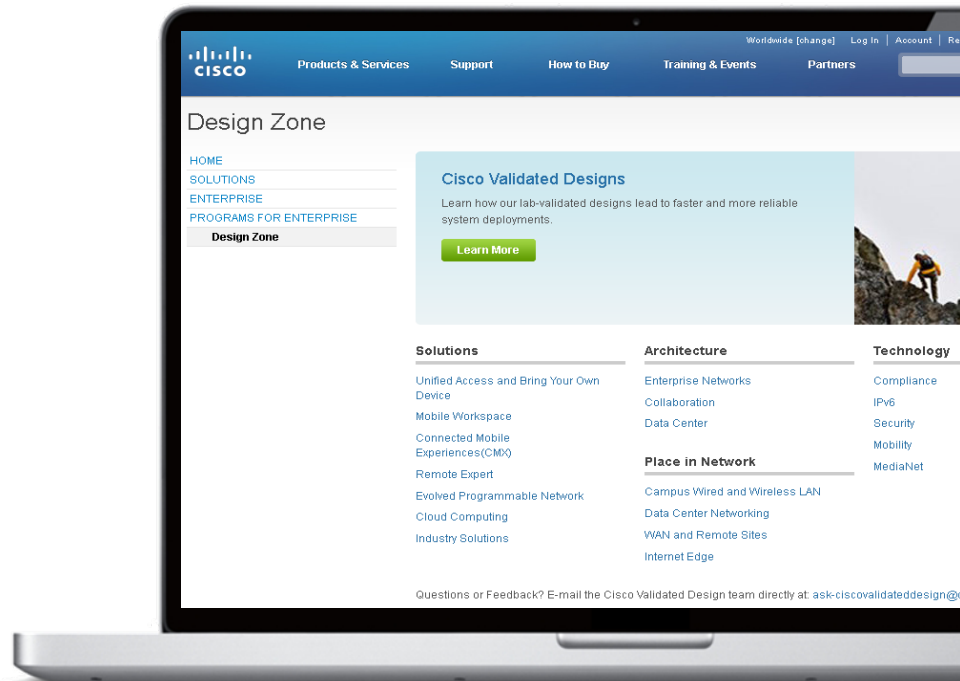
Обзорные документы

Документы At-a-Glance

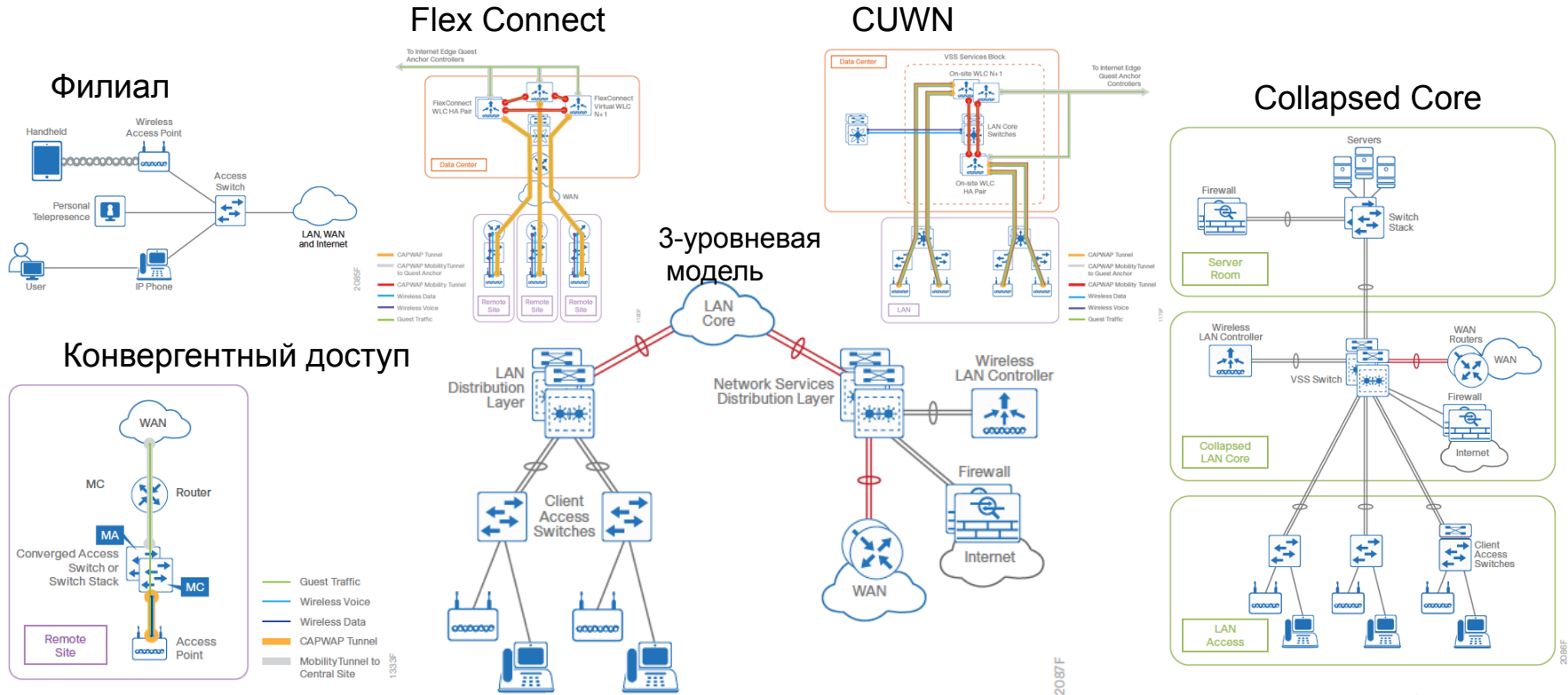
Презентации

www.cisco.com/go/cvd

www.cisco.com/go/cvd/campus



Reference Network Architecture



Рекомендации в зависимости от размера сети



Крупное
предприятие

Ядро с 3-мя и более
блоками
распределения

“3-х уровневая модель”

Сеть средних
размеров

Распределение с 2-
мя и более блоками
доступа

“2-х уровневая модель”
или Collapsed Core

Филиал,
небольшое
предприятие

Один блок доступа

Примерно:
< 100 точек доступа
< 250 пользователей

Рекомендации в зависимости от функционала



Enterprise Class

“Хорошо”

Базовые сетевые сервисы

Примеры: 1 Gigabit Ethernet access, PoE+, 802.11ac до 1 Гбит/с, 3x3 MIMO:2SS, CleanAir Express, Transmit Beamforming

Mission Critical

“Лучше”

Базовые сервисы и дополнительные возможности

Примеры: 1/10/40 Gigabit Ethernet, MACsec, TrustSec (распределение/Instant Access), NetFlow, UPOE, 802.11ac более 1 Гбит/с, 3x4 MIMO:3SS, HDX, CleanAir 80 MHz, ClientLink 3.0, VideoStream

Best in Class

“Самое лучшее”

Широкий выбор передовых сервисов

Примеры: очень высокая доступность, 1/10/40/100 Gigabit Ethernet, MACsec, TrustSec (распределение/Instant Access), NetFlow, UPOE, 802.11ac более 1 Гбит/с, 4x4 MIMO:3SS, HDX, CleanAir 80MHz, ClientLink 3.0, Video-Stream, модульность для 3G/Location/Wave 2

Reference network architecture



Размер	Роль	<div style="display: flex; justify-content: space-between; align-items: center;"> Enterprise Class Mission Critical Best in Class </div> <div style="display: flex; justify-content: center; align-items: center; margin-top: 5px;"> “хорошо” ← Функциональность → “самое лучшее” </div> <div style="display: flex; justify-content: space-between; font-size: 0.8em; margin-top: 5px;"> Базовые сетевые сервисы Базовые сервисы и дополнительные возможности Широкий выбор передовых сервисов </div>		
		крупный	Ядро	6807-XL (опц. VS40) или Nexus 7700
Распр.	3850 Fiber Stack SSO		6880-X VSS	6807-XL VS40
Доступ	2960-X		3850/3650 или 6800IA	4500E Sup8E SSO
БЛВС / ТД	Централизованный 5500 HA SSO / 1700		Централизов. 8500/5500 HA SSO / 2700	Централизов. 8500 HA SSO / 3700
Распр.	3850 Fiber Stack SSO		4500E Sup8E VSS	6880-X VSS
средний	Доступ	2960-X	3850/3650	3850
	БЛВС / ТД	Flex Connect 8500/7500/5500 HA / AP1700	3K Converged Access/AP2700	3K Converged или 5500/2500 /AP3700
	Распр.	3850 Fiber Stack SSO	4500E Sup8E VSS	6880-X VSS

Программа

Задачи презентации

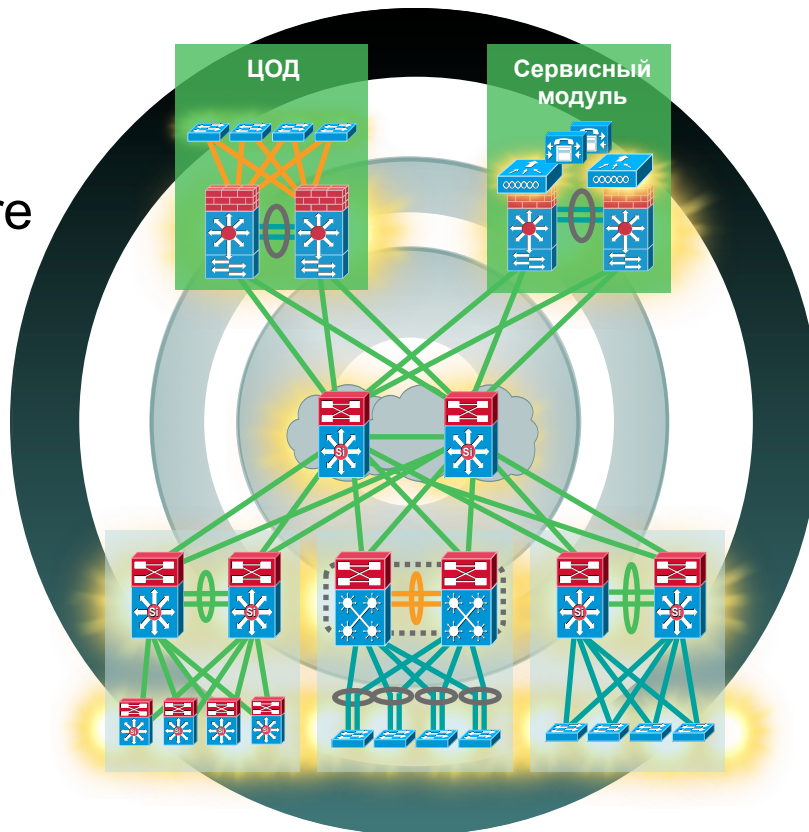
Обзор ключевых сервисов

Reference Network Architecture

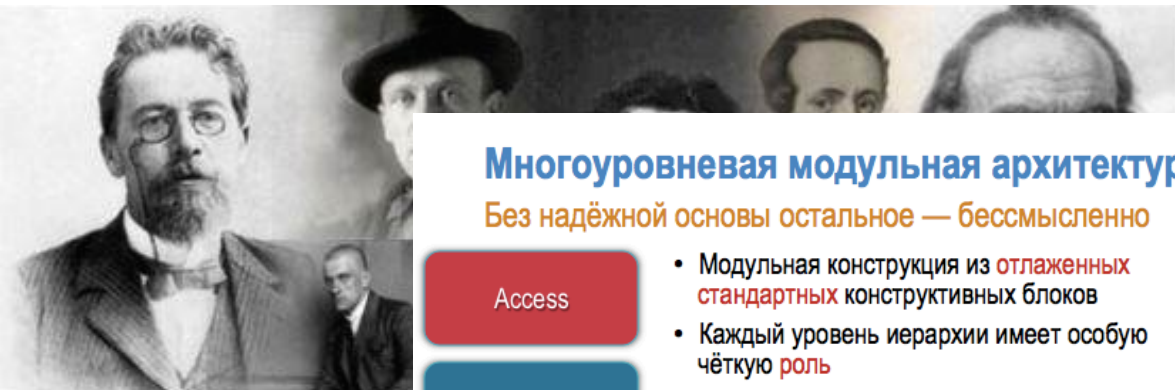
Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- Converged Access
- Instant Access

Заключение



Классика...



Многоуровневая модульная архитектура ЛВС

Без надёжной основы остальное — бессмысленно

Access

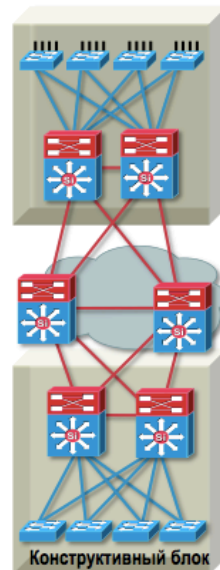
Distribution

Core

Distribution

Access

- Модульная конструкция из **отлаженных стандартных** конструктивных блоков
- Каждый уровень иерархии имеет особую чёткую **роль**
- Легко понимать, сопровождать, ремонтировать, расширять, улучшать
- Компактные **домены отказов** изолированы чёткими границами
- Стимулирует **балансировку** трафика и **резервирование** в условиях избыточности
- Способствует **детерминизму** поведения
- Накладывает протоколы на физическую и логическую топологию
- Использует **маршрутизацию** для балансировки, быстрого восстановления, надёжности, управляемости



Уровень доступа

Новые
возможности
доступа с mGig!

■ Доступ к сети

- Проводной 10/100/1000
- Беспроводной 802.11a/b/g/n/ac

■ Простой и гибкий дизайн

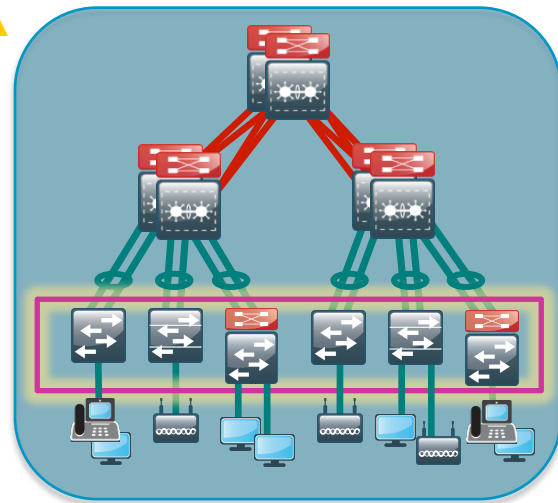
- Граница L2 для приложений, требующих растянутых VLAN
- По возможности исключить необходимость в Spanning Tree

■ Точка применения политик

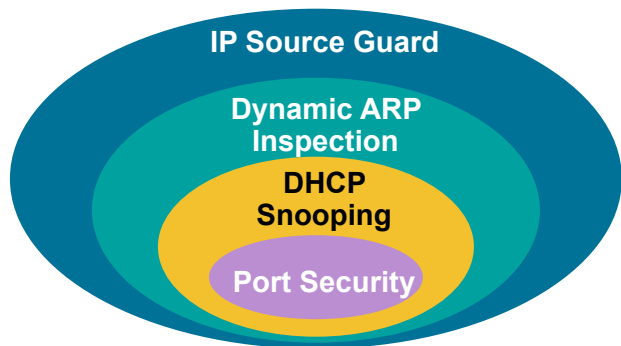
- Защита сети и приложений от атак
- Маркировка QoS

■ Поддержка расширенного функционала

- Поддержка PoE: 802.3af(PoE), 802.3at(PoE+), Cisco Universal POE (UPOE) – 60 Вт
- Обеспечение QoS для приложений
- Netflow



Уровень доступа – защита границы



Рекомендации Cisco Validated Design: использовать встроенные функции коммутаторов Catalyst для защиты сети от целенаправленных и **непреднамеренных** атак

- **Port security:** предотвращает атаки на таблицу CAM и истощение DHCP
- **DHCP Snooping:** предотвращает атаки с использованием нелегитимных DHCP серверов
- **Dynamic ARP Inspection:** предотвращает атаки на ARP
- **IP Source Guard:** предотвращает спуфинг IP/MAC

Рекомендации по обеспечению отказоустойчивости

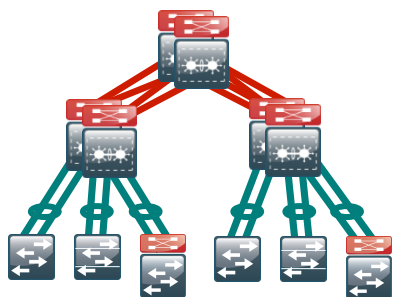
Rapid PVST+ усовершенствованные механизмы обнаружения изменений в топологии

BPDUGuard default – обнаружение BPDU на портах с настроенным portfast

UDLD – обнаружение и защита от однонаправленных соединений

Error disable recovery – возможность автоматического восстановления портов

VTP transparent – защита от непреднамеренного изменения списка VLAN



```
spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
udld enable
errdisable recovery cause all
vtp mode transparent
load-interval 30
```

Уровень распределения

Основная функция – агрегация каналов уровня доступа в здании или определенной области

Отказоустойчивый дизайн для уменьшения последствий возможных неполадок в сети

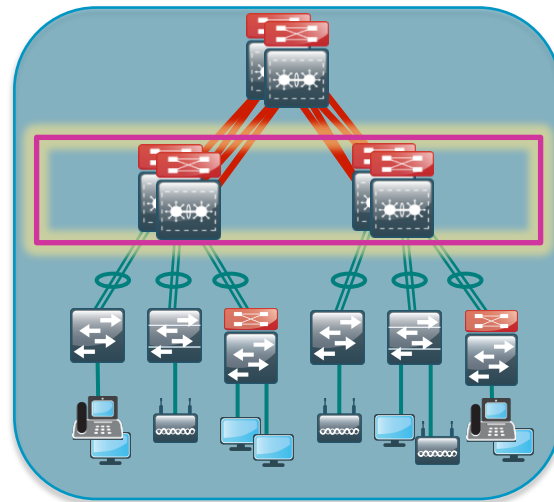
Граница L2 для уровня доступа

- Граница Spanning Tree Protocol
- Разграничение широковещательных доменов
- Балансировка нагрузки

Функциональность L3

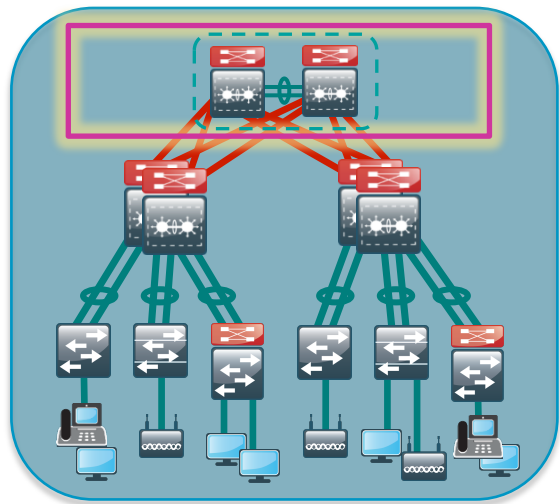
- Шлюз по умолчанию и FHRP
- Агрегирование маршрутной информации
- Эффективный IP Multicast
- балансировка трафика по параллельным каналам в магистраль

Необходимость в QoS, связанная с агрегированием каналов



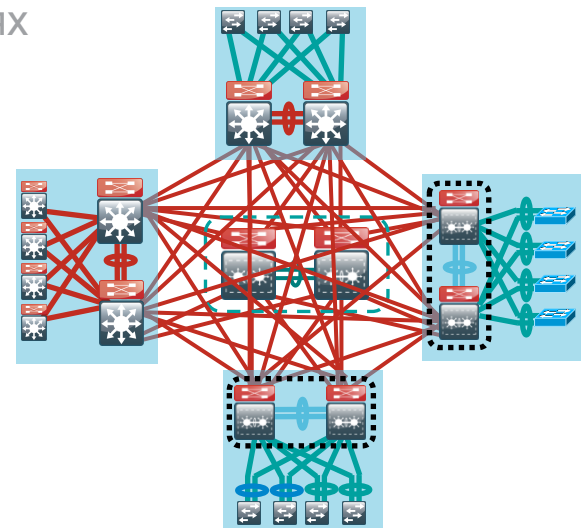
Уровень ядра

- Основа всей сети – объединяет конструктивные блоки. Связывает уровни распределения в распределенных сетях
- Снижает стоимость и сложность полносвязных топологий

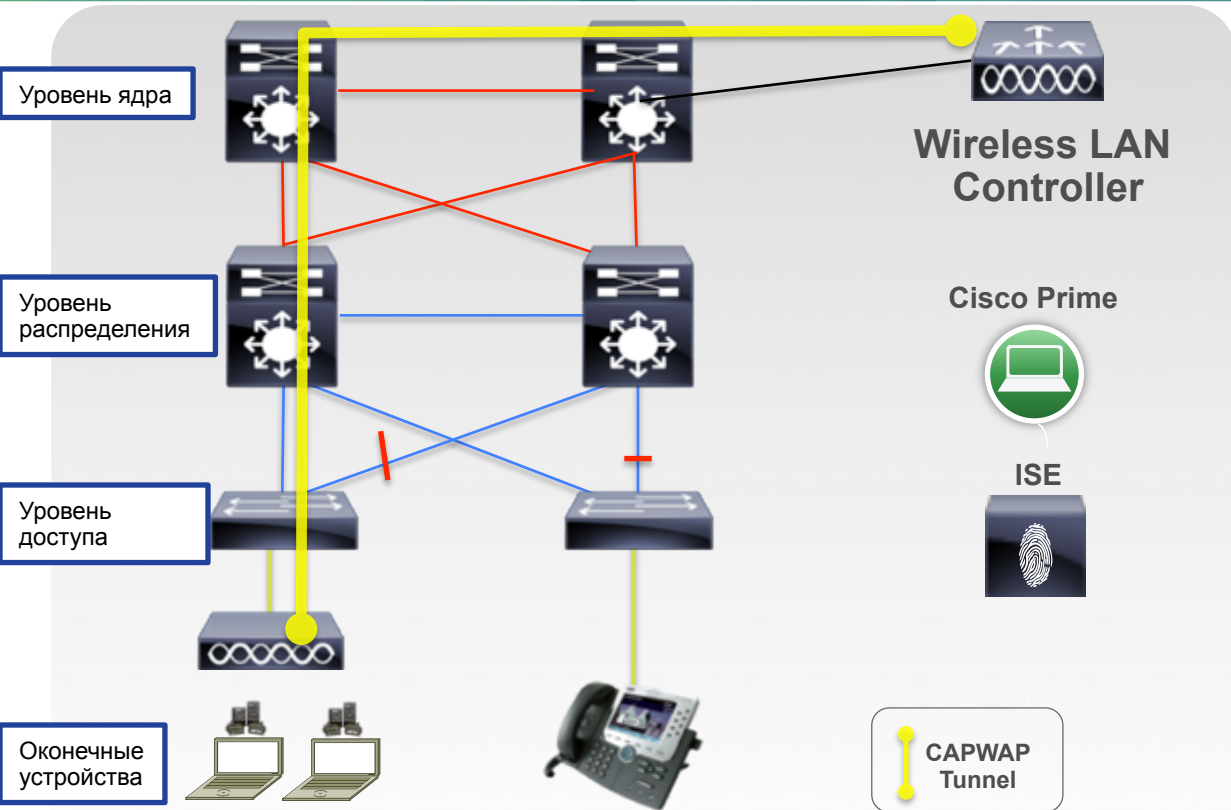


- Высокая отказоустойчивость – дизайн без единых точек отказа
- Максимальная простота и унификация
 - Исключить необходимость постоянного тюнинга и внесения изменений в конфигурацию
- Транспорт Layer 3
 - Исключить Spanning Tree и заблокированные порты

Нужен ли мне уровень ядра?



Традиционный доступ – Многоуровневый дизайн



Многоуровневый дизайн ЛВС

Особенности

Сетевой дизайн с высокой надёжностью

Необходим тюнинг протоколов L2/L3

Необходимо соответствие поддерживаемых протоколов

Гибкость внедрения

Хорошо известный и понятный дизайн

Характеристики многоуровневой модели дизайна

Преимущества

Хорошо понятный и хорошо задокументированный типовой дизайн с многолетней историей успешных внедрений

Использует индустриальные стандарты протоколов, таких как Rapid Spanning Tree Protocol и т.д.

Отличительные особенности и возможности на базе решений Cisco (PVST+), обеспечивающие быструю сетевую конвергенцию в пределах 1 секунды

Возможность использования оборудования различных производителей

Гибкий выбор широкого спектра оборудования различной стоимости

Недостатки

Требуется трудоёмкая конфигурация и тюнинг для достижения быстрой сетевой конвергенции в пределах 1 секунды

Появляется дополнительная сложность в эксплуатации при добавлении VLAN или VRF сегментации

Все коммутаторы управляются индивидуально

Комплексные задачи – требуется настройка и тюнинг Spanning Tree, маршрутизации, отказоустойчивость шлюза по умолчанию

Поиск и устранение неисправностей Spanning Tree

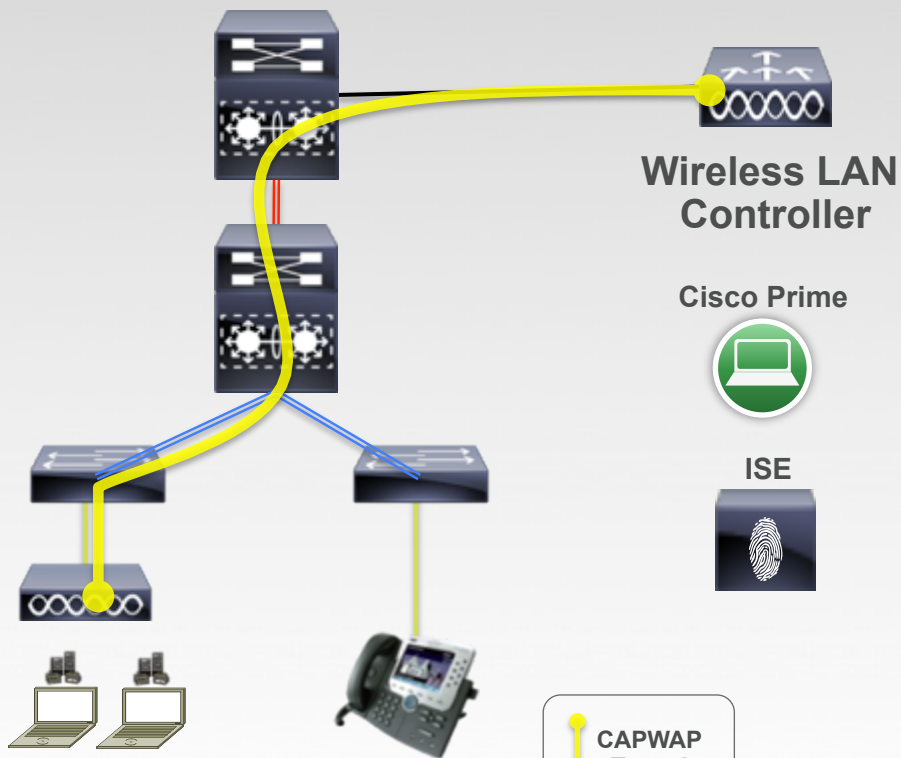
Традиционный доступ – Virtual Switching System

Уровень ядра

Уровень распределения

Уровень доступа

Оконечные устройства



VSS CAMPUS DESIGN

Особенности

Упрощение тюнинга протоколов

Более эффективное использование ресурсов

Более высокая гибкость с использованием Quad Sup VSS

Уменьшение кол-ва Routing Peers

Некоторые заказчики предпочитают отдельные control plane

Характеристики модели дизайна с VSS

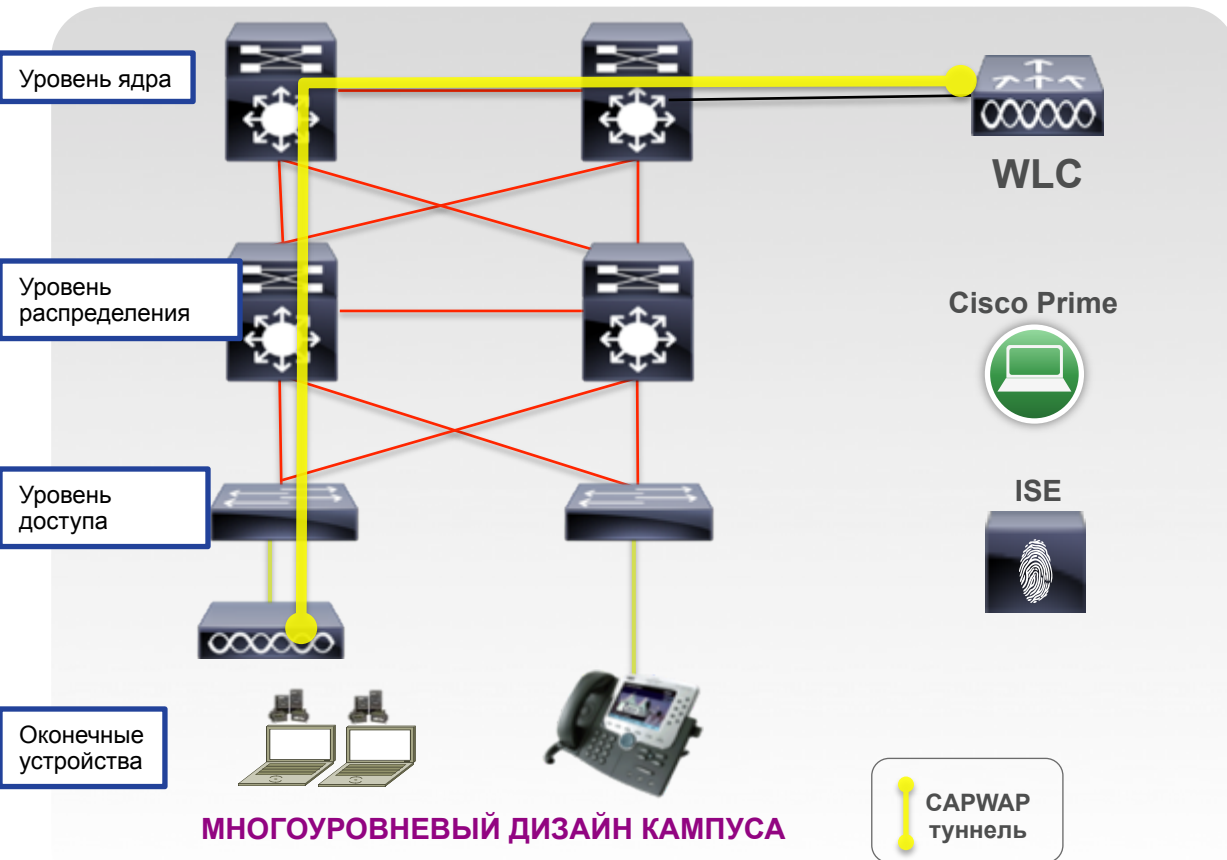
Преимущества

- Упрощённый сетевой дизайн с объединением двух физических устройств в одну логическую единицу
- Нет необходимости в First Hop Redundancy Protocol
- Etherchannel-трафик распределяется и балансируется между несколькими аплинками
- Обеспечивает возможность расширения L2-домена с распределением VLAN'ов на нескольких коммутаторах доступа без заблокированных каналов STP
- Поддерживает сетевую конвергенцию в пределах 1 секунды
- Возможность использования оборудования различных производителей на доступе
- Коммутаторы распределения управляются как одна логическая единица

Недостатки

- Решение разработано Cisco, требуются коммутаторы Cisco на уровнях ядра/распределения
- Коммутаторы доступа управляются индивидуально
- Использование единой control plane нежелательно для некоторых заказчиков
- Нет отличительных особенностей и возможностей на базе решений Cisco, обеспечивающих быструю сетевую конвергенцию в пределах 1 секунды

Традиционный доступ – дизайн на основе маршрутизируемого доступа



Особенности

Единая Control Plane

Упрощенное восстановление сети

Использование дополнительных IP-адресов

VLAN's распространяются до WLC

Широкий выбор средств диагностики

Характеристики модели внедрения маршрутизируемого доступа

Преимущества

- Единая control plane = уменьшение сложности
- Меньше необходимость в тюнинге протоколов для ускорения сходимости (зависит от протокола)
- Развитый набор средств диагностики
- Использование настроек ECMP по-умолчанию для эффективного использования доступных соединений и быстрой сходимости
- Нет необходимости в протоколах FHRP (HSRP/VRRP)
- Нет необходимости в транках
- Возможность повторного использования VLAN ID
- Упрощение мультикаст-топологии

Недостатки

- Необходимость в дополнительных IP-адресах (усложнение схемы IP-адресации)
- VLAN'ы ограничены в рамках одного коммутатора – нет возможности распространить VLAN'ы между разными коммутаторами и расширить L2-домен
- Может потребоваться тонкая настройка ECMP / CEF hash для наиболее эффективного использования связей в топологии (на старом оборудовании)
- Нет возможности сделать RSPAN (рекомендуется ER-SPAN)

Основные платформы для традиционного доступа

Ядро/
распределение



6880-X



6840-X



4500-X



3850-XS



Catalyst 6500-E



Catalyst 6807-XL



Nexus 7700

Доступ



2960



3650



3850



Catalyst 4500-E Sup8E

Фиксированные

Модульные

Фиксированные платформы 10G/40G

New

10G Fiber Agg 3850-XS



- **C3850-12XS** или **24XS**
 - NM-8-10G или NM-2-40G
 - Поддержка стека (8) + SSO
- **C3850-48XS**
 - Встроенные 4 x QSFP
 - Нет STACK / SSO
- **L2 / L3: 32K MAC / 24K IP**

10G Fiber Agg 4500-X



- **C4500-X-16P**
- **C4500-X-32P**
- NM-8-10G
- Только SFP / SFP+
- VSS + SSO
- **L2 / L3: 55K MAC / 256K IP**

New

10G Fiber Agg & Core 6840-X



- **C6816-X-LE**
- **C6824-X-LE-40G**
- **C6832-X-LE**
- **C6840-X-LE-40G**
- VSS + IA + SSO
- **L2 / L3: 128K MAC / 256K IP**

10G Fiber Agg & Core

6880-X



- **C6880-X**
- **C6880-X-LE**
- до 4 C6880-X-16P10G
- Только SFP / SFP+
- VSS + IA + SSO
- **L2 / L3: 128K MAC / 2M IP**

Enterprise

Mission Critical

Best In Class



Модульные платформы 10G/40G

10G / 40G Agg 6500-E



- **WS-X6904-40G**
 - Встроенные 4 x CFP (SR4 & LR4)
 - До 16 x SFP/SFP+ (с CVR)
- **C6800-32P10G**
 - Встроенные 32 x SFP/SFP+
 - До 8 x QSFP (w/ CVR*)
- **L2 / L3: 128K MAC / 1M IP**

10G / 40G Agg & Core 6807-XL



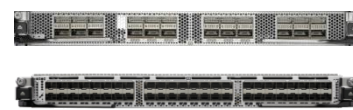
- **WS-X6904-40G**
 - Встроенные 4 x CFP (SR4 & LR4)
 - До 16 x SFP/SFP+ (с CVR)
- **C6800-32P10G**
 - Встроенные 32 x SFP/SFP+
 - До 8 x QSFP (с CVR*)
- **L2 / L3: 128K MAC / 1M IP**

10G / 40G Core 7000



- **N7K-M206FQ-23L**
 - 6 x QSFP
- **N7K-M224XP-23L**
 - 24 x SFP/SFP+
- **L2 / L3: 128K MAC / 1M IP**

10G / 40G Core 7700



- **N77-F324FQ-25**
 - 24 x QSFP
- **N77-F348XP-23**
 - 48 x SFP/SFP+
- **L2 / L3: 64K MAC / 64K IP**

Защита инвестиций: адаптер 10G -> 40G



C6800-32P10G



C6800-16P10G



C6800-8P10G



6880-X



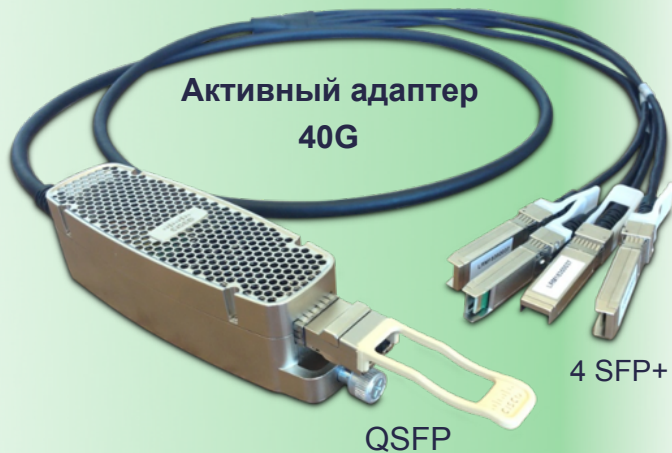
6840-X



SUP8-E



4500-X



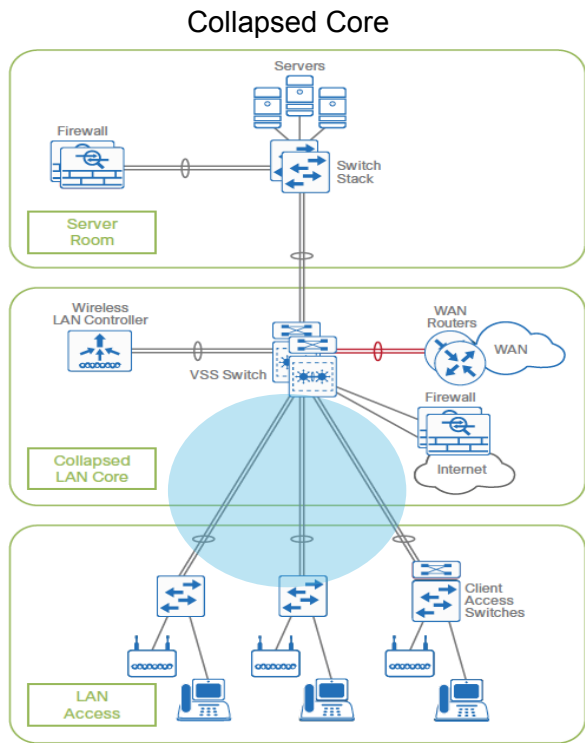
10GE сейчас

40GE позже

QSFP-40G-SR4
QSFP-40G-CSR4
QSFP-40G-SR-BD
QSFP-40G-LR4
QSFP-40G-ER4

Каналы 10 Гбит в распределение/ядро

10G Downlink



3850-XS for Low-Med Density 10G & Good Core Features

- Up to 8 x 3850-12/24XS per Stack
- 12-24 x 10G per 3850-XS, 96-192 with 8 Stack
- **Stacking + SSO – Cross-Connect (4) DEC to Access**

4500-X / 4500-E for Low-Med 10G & Better Core Features

- 32 x 10G per 4500-X, 64 x 10G with VSS
- 96 x 10G per 4510-R+E (8 x 4712-SFP), 192 with VSS
- **Redundant Sup + SSO – Dual-Home (2-4) DEC to Access**
- **VSS + SSO – Cross-Connect (4) MEC to Access**

6800-X / 6807-XL for Med-High 10/40G & Best Core Features

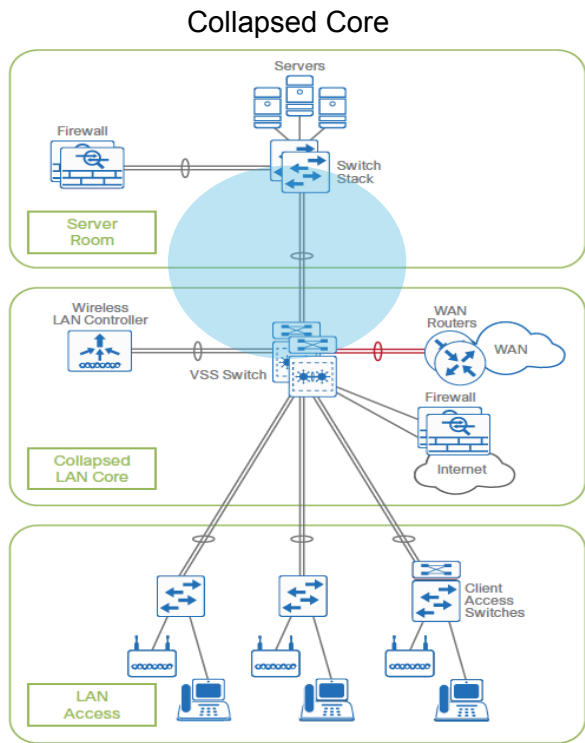
- 40 x 10G per 6840-X, 80 x 10G with VSS
- 80 x 10G per 6880-X, 160 x 10G with VSS
- 160 x 10G per 6807-XL (5 x 32P10G), 320 with VSS
- **Redundant Sup + SSO – Dual-Home (2-4) DEC to Access**
- **VSS + SSO – Cross-Connect (4) MEC to Access**

N7004 / N7706 for High 10/40G & Good Core Features

- 96 x 10G per N7004 (4 x M224XP)
- 192 x 10G per N7706 (4 x F348XP)
- **Redundant Sup + SSO – Dual-Home (2-4) DEC to Access**

Каналы 40 Гбит в ядро/ЦОД

40G Uplink Considerations



3850-XS for Low Density 40G with Good Core Features

- Up to 8 x 3850-24XS per Stack
- 2 x 40G per 3850-24XS (NM), 16 with 8 Stack
- **Stacking + SSO – Dual-Home (2) DEC to Dist/DC**

4500-X / 4500-E for Low 40G with Better Core Features

- 2 x 40G per 4500-X (Uplink/CVR*), 4 with VSS
- 4 x 40G per 4510-R+E (Sup8/CVR*), 8 with VSS
- **Redundant Sup + SSO – Dual-Home (2) DEC to Dist/DC**
- **VSS + SSO – Cross-Connect (4) MEC to Dist/DC**

6800-X / 6807-XL for Low-Med 40G with Best Core Features

- 2-6 x 40G per 6840-X (Uplink/CVR*), 4-12 with VSS
- 20 x 40G per 6880-X (w/CVR*), 40 with VSS
- 40 x 40G per 6807-XL (5 x 32P10G w/CVR*), 80 with VSS
- **Redundant Sup + SSO – Dual-Home (2-4) DEC to Dist/DC**
- **VSS + SSO – Cross-Connect (4) MEC to Dist/DC**

N7009 / N7710 for High 40G with Good Core Features

- 54 x 40G per N7004 (9 x M206FQ)
- 192 x 40G per N7706 (8 x F324FQ)
- **Redundant Sup + SSO – Dual-Home (2-4) DEC to Dist/DC**

Программа

Задачи презентации

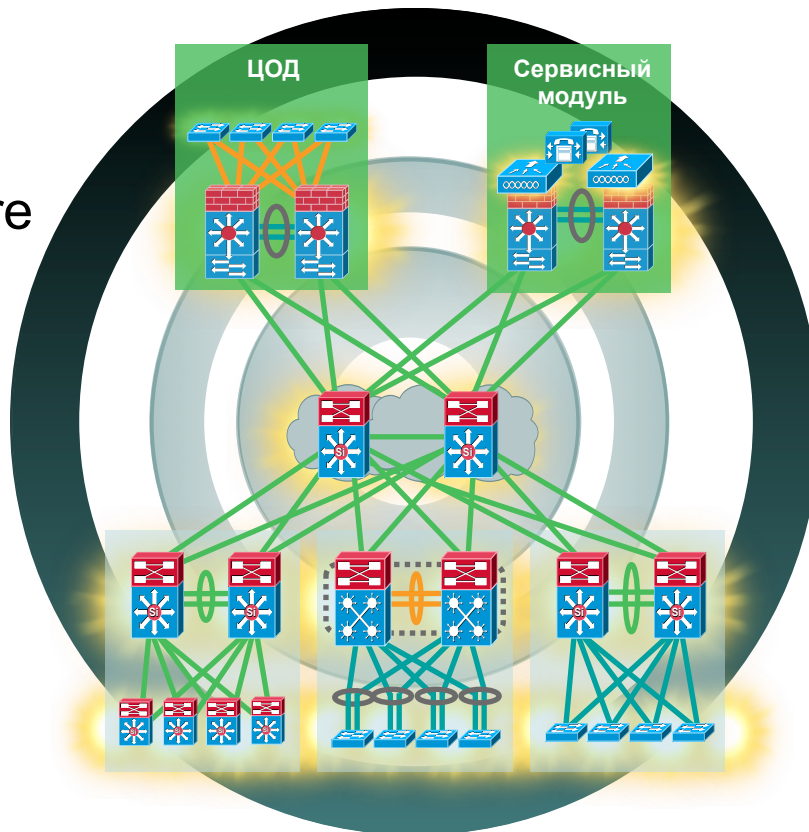
Обзор ключевых сервисов

Reference Network Architecture

Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- **Converged Access**
- Instant Access

Заключение



Конвергентный доступ

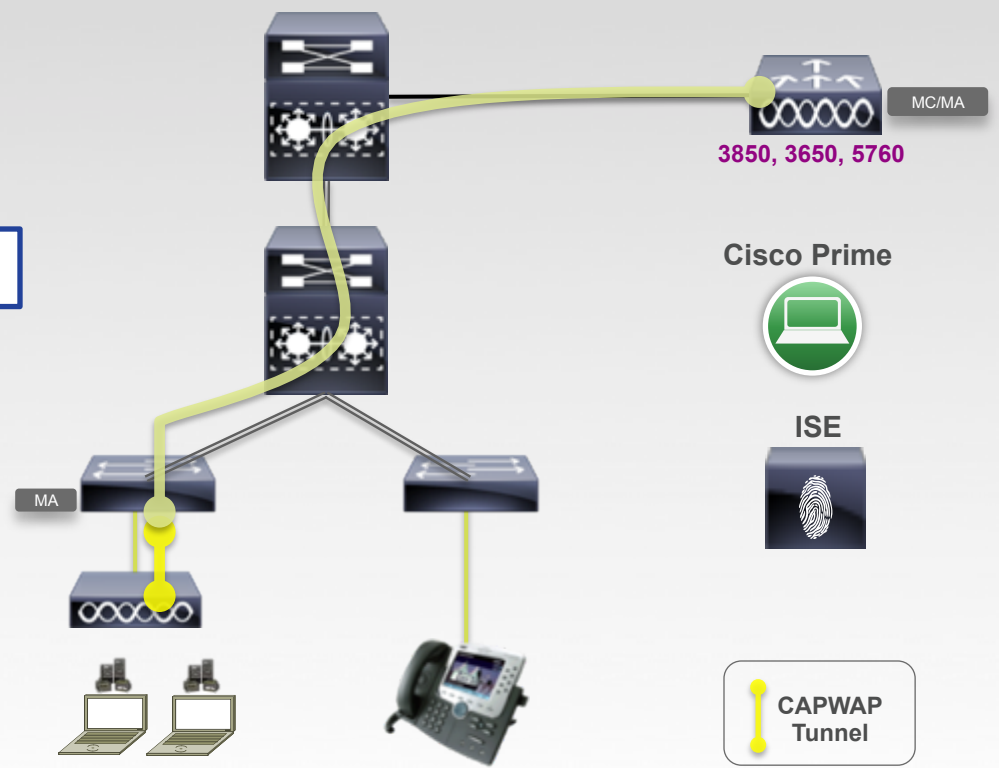


Уровень ядра

Уровень распределения

Уровень доступа

Оконечные устройства



Многоуровневая модель, VSS, или маршрутизируемый доступ

Особенности

Единая модель QoS для проводных/беспроводных подключений

Прозрачность беспроводного трафика

Единые сервисы для проводных/беспроводных подключений

Отсутствие необходимости в выделенном контроллере для решений с менее 250 ТД

Полная поддержка 802.11ac

Поддержка многоуровневой модели или маршрутизируемого доступа

Характеристики конвергированного доступа

Преимущества

Может внедряться в существующую традиционную архитектуру для упрощения миграции

3850/3650/4500E могут терминировать CAPWAP как Mobility Agent совместно с традиционными контроллерами 3850, 3650, 5760 в роли Mobility Controller

Единая модель QoS для проводных/ беспроводных подключений на 3850/3650/4500E

Поддержка Flexible Netflow для проводных/ беспроводных подключений

Более эффективное использование мультикаста за счет терминирования CAPWAP на коммутаторе доступа

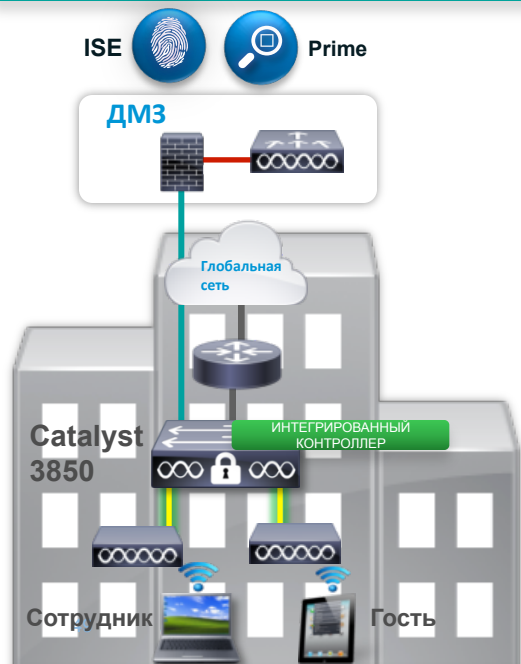
Недостатки

Распределенное управление и диагностика для беспроводной сети

Неполное соответствие функционала AireOS и IOS XE

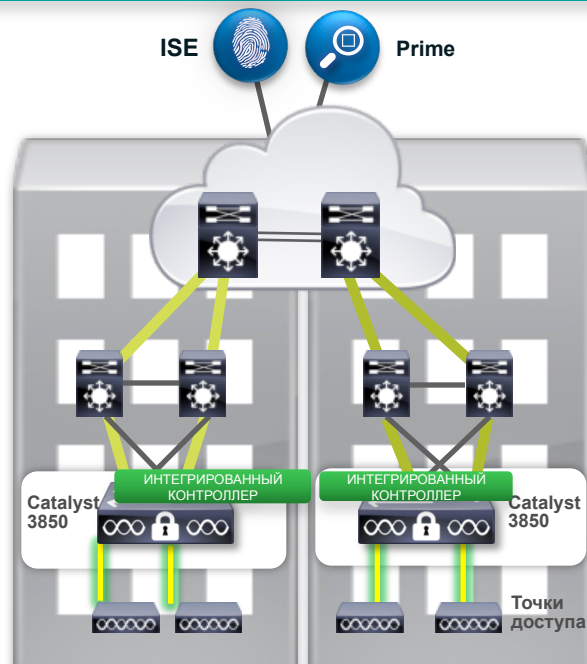
Режимы развертывания конвергированного доступа На примере Catalyst 3850

ВОЗМОЖНОСТИ ИНТЕГРИРОВАННОГО КОНТРОЛЛЕРА



ФИЛИАЛ

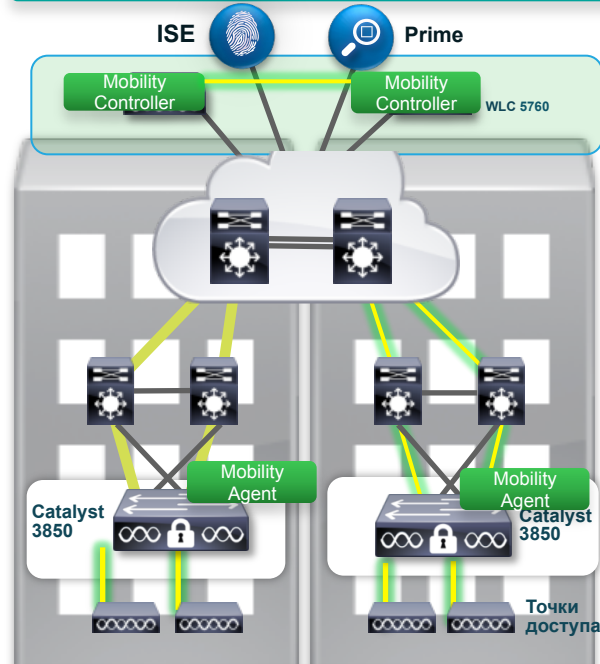
ДО 50-100 ТОЧЕК ДОСТУПА



НЕБОЛЬШОЙ ИЛИ СРЕДНИЙ КОМПЛЕКС
ЗДАНИЙ

ДО 200 ТОЧЕК ДОСТУПА

ВНЕШНИЙ КОНТРОЛЛЕР MOBILITY CONTROLLER



КРУПНЫЙ КОМПЛЕКС ЗДАНИЙ

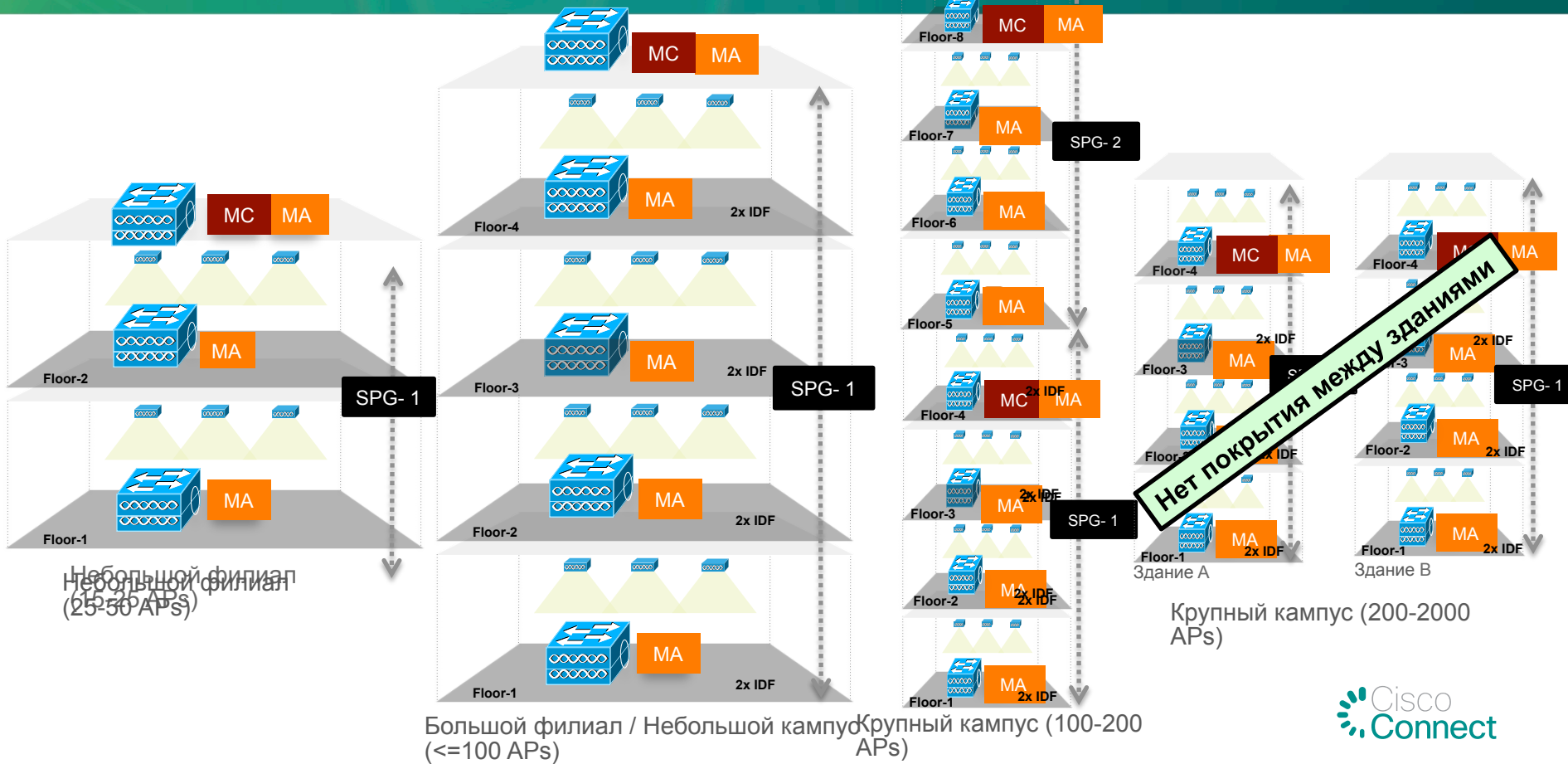
>200 точек доступа

Туннель CAPWAP

Стандартное подключение Ethernet, без туннелей

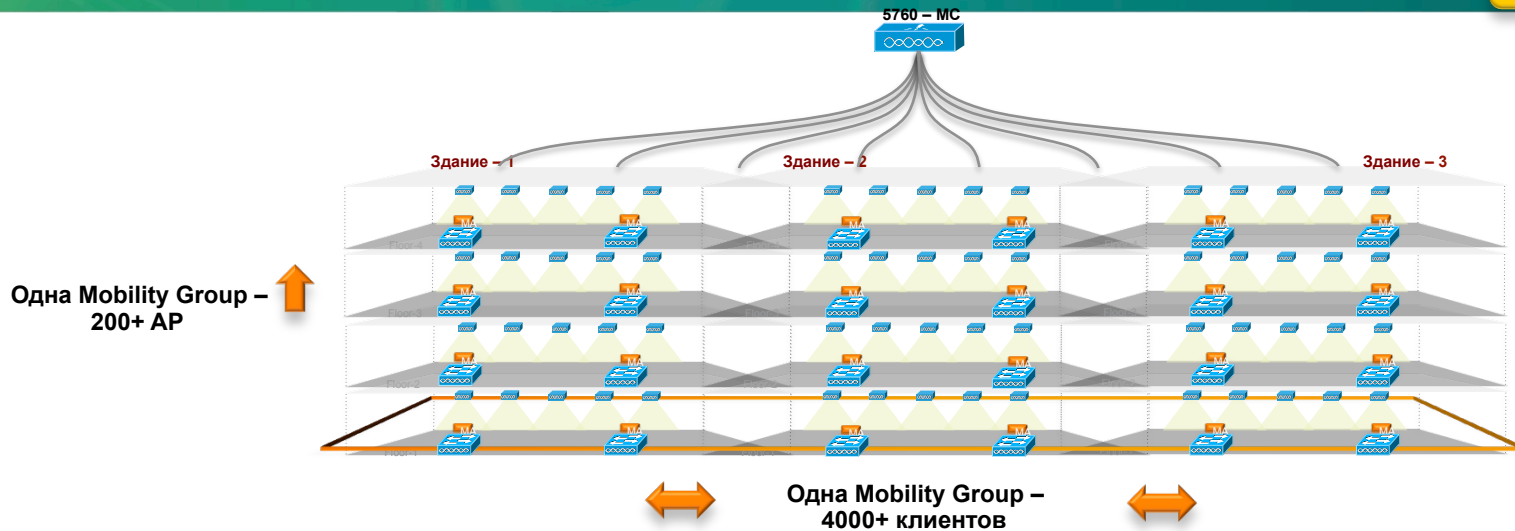
Гостевой туннель от коммутатора к контроллеру DMZ

Конвергированный доступ



Конвергированный доступ – внешний контроллер

5760 – рекомендованное ПО:
IOS-XE 3.6.3



- Использование внешнего контроллера, когда MC на базе коммутаторов Catalyst не могут поддерживать следующие масштабы:
 - Единый домен с 200+ точками доступа, полное покрытие
 - Прозрачный роуминг для 4000+ устройств между всеми точками доступа

Конвергированный доступ. Сценарии

Прозрачный роуминг

Mobility Domain – > 7000 Устройств / > 600 ТД
Centralized Overlay

Mobility Domain 7000 Устройств / 600 ТД
5760 MC

3

5%



Mobility Domain 4000 Устройств / 100 ТД
Max 2 x 3850 MC

2

5%

Mobility Domain – до 2000 Устройств / 50 ТД
Max 1 x 3850 MC

1

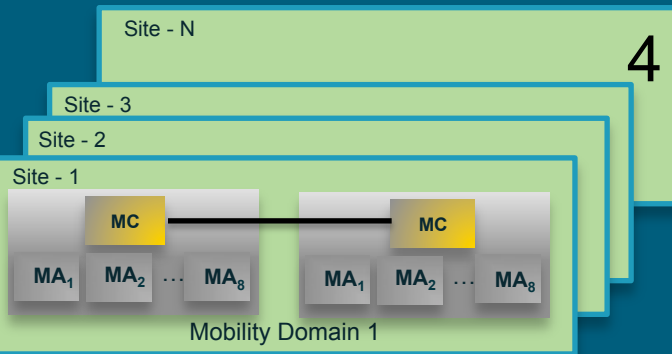
88%

Размер домена

Независимые домены мобильности

(N) X независимых Mobility Domain
Up to 4000 Devices / 100 AP's per Mobility Domain

2%



Количество устройств

Размер домена

Основные платформы для конвергированного доступа

Ядро/
распределение



6880-X



6840-X



4500-X



3850-XS



Catalyst 6500-E



Catalyst 6807-XL



Nexus 7700

Доступ



3650



3850



Catalyst 4500-E Sup8E

Фиксированные

Модульные

Программа

Задачи презентации

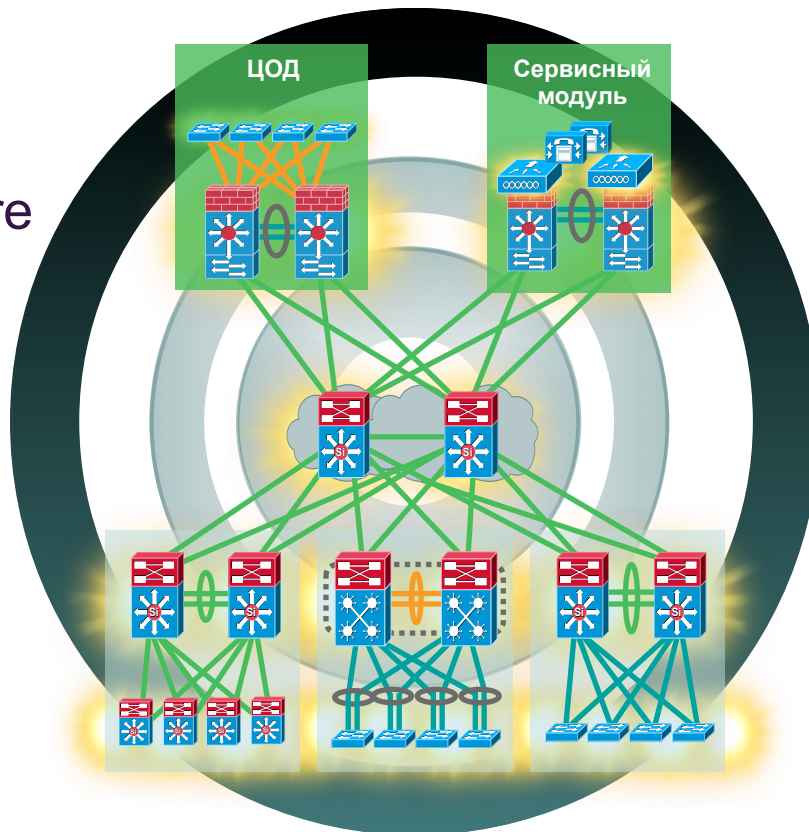
Обзор ключевых сервисов

Reference Network Architecture

Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- Converged Access
- **Instant Access**

Заключение

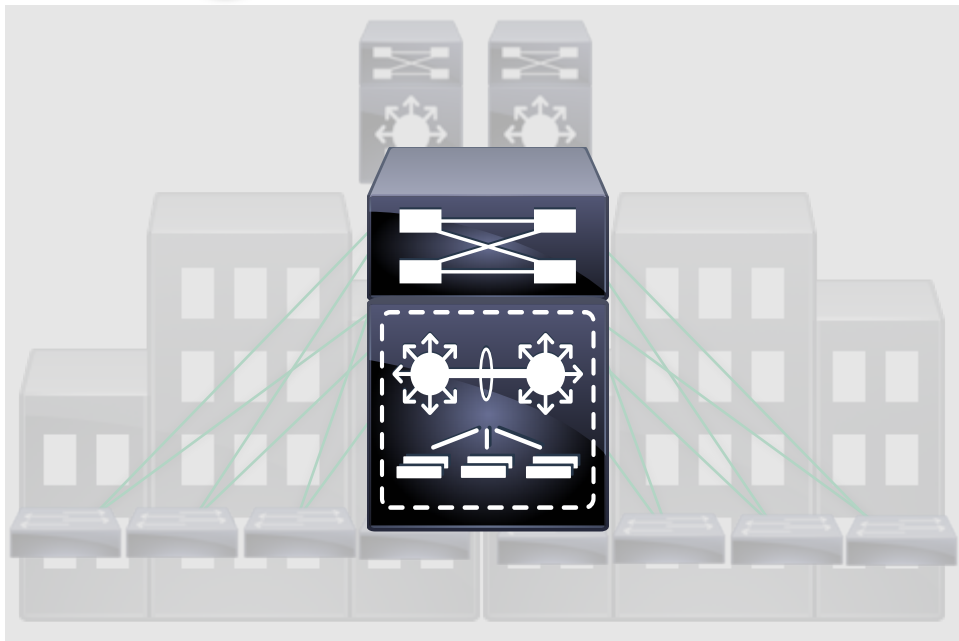


Технология Instant Access

ISE Cisco Prime



Количество управляемых устройств > 20



Блок сети кампуса на 1500/2000 портов

Особенности

Поддержка технологий **Stacking, POE+** на уровне доступа

Единая точка **управления, настройки и поиска неисправностей**

Упрощенный дизайн для VLAN и агрегированных каналов

Гибкая инфраструктура позволяет добавлять **новый функционал** единообразно для всего **уровня доступа**

Единый образ **IOS внедрения и управления** для всего блока

УМЕНЬШЕНИЕ ТСО

Масштабирование Instant Access

Функциональность	SUP2T			6880-X		6840-X
	15.1(2)SY (Shipping)	15.2(1)SY (Shipping)	15.2(1)SY1 (Shipping)	15.1(2)SY (Shipping)	15.2(1)SY (Shipping)	15.2(2)SY (Sep'15)
Количество портов	1,000	1,200	1,500	1,000	2,000	1,500*
Fabric Link – 6800ia	12	25	32	12	42	32
Fabric Link – 3560CX	n/a	42	42	n/a	42	n/a*
Стекирование	3	5	5	3	5	5

*At FCS

Характеристики технологии Instant Access

Преимущества

- Единая точка управления, конфигурации и диагностики для блока распределения
- Упрощение дизайна блока распределения упраздняет необходимость конфигурирования аплинков
- Простое управление ПО на коммутаторах
- Надежность и функционал Catalyst 6500/6800 на уровне доступа
- Может совместно использоваться с традиционным или конвергированным доступом
- Решение для заказчиков с поддержкой MPLS и других расширенных функций на уровне доступа

Недостатки

- Ограничение одного блока распределения – 1500/2000 портов
- Большое количество east-west трафика может увеличить загрузку аплинков (переподписка)
- Поддержка только в VSS конфигурациях (поддерживается один коммутатор в режиме VSS)
- Различия в функционале уровня доступа между Cat6k и традиционными Cat2k/3k/4k
- Нет возможности терминировать CAPWAP-туннели на портах клиентских коммутаторов Instant Access

Catalyst Instant Access

Ключевые компоненты

INSTANT ACCESS РОДИТЕЛЬСКОЕ УСТРОЙСТВО

Catalyst 6500E



Sup 2T



6904



FourX



Catalyst 6807-XL



Sup 2T



6904



FourX



Catalyst 6880-X



INSTANT ACCESS КЛИЕНТСКОЕ УСТРОЙСТВО

Catalyst 6848ia



Беспрецедентное сохранение инвестиций!



Основные платформы для Instant Access

Магистральи



6880-X



6840-X



Catalyst 6500-E



Catalyst 6807-XL

Доступ



Catalyst 6800ia



C3560CX-8XPD-S
(15.2(1)SY)

ОТСУТСТВУЮТ

Фиксированные

Модульные

Программа

Задачи презентации

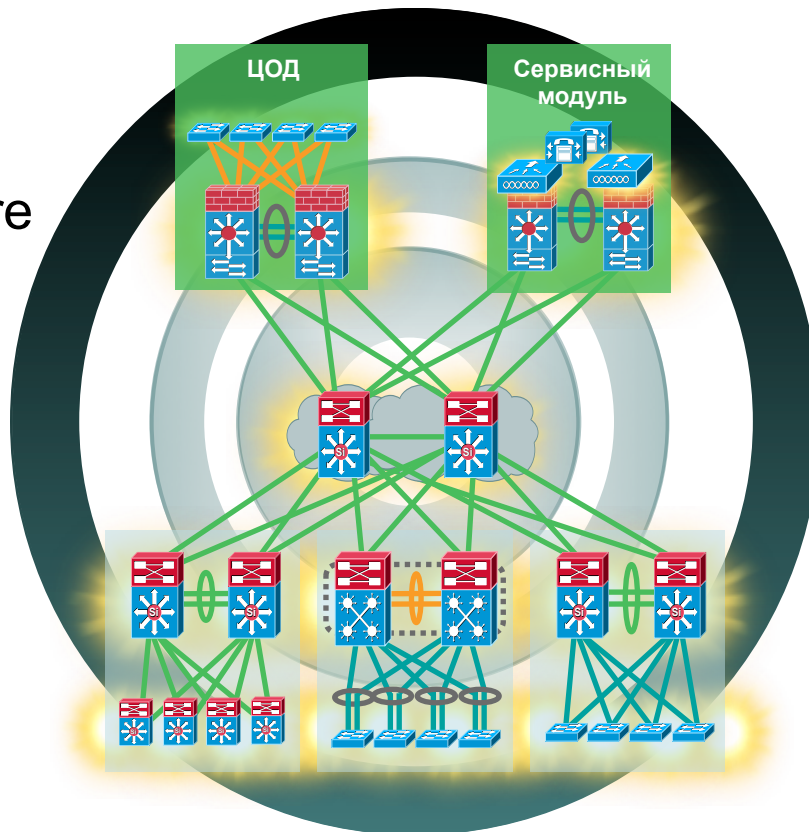
Обзор ключевых сервисов

Reference Network Architecture

Модели дизайна

- Традиционный доступ
 - Многоуровневый
 - Маршрутизируемый
 - VSS
- Converged Access
- Instant Access

Заключение



Модели внедрения доступа

Cisco Prime



ISE



WiSM725508

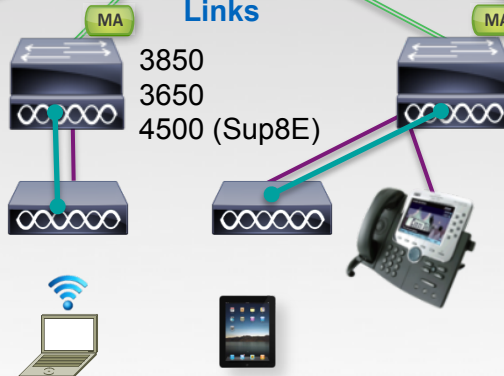
L2/L3 Links



2960-X
3650
3850
4500 (Sup8E)

ТРАДИЦИОННЫЙ ДОСТУП

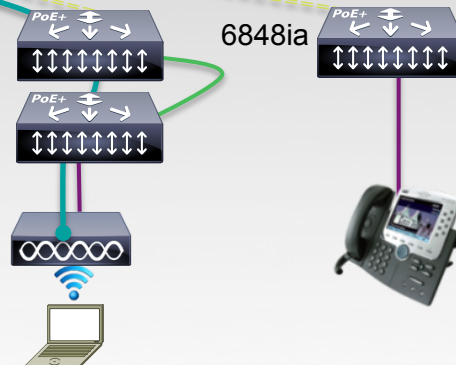
L2/L3 Links



3850
3650
4500 (Sup8E)

КОНВЕРГИРОВАННЫЙ ДОСТУП

Fabric Links



6848ia

INSTANT ACCESS

CAPWAP Tunnel

Wireless

Централизованный

Распределенный

Централизованный

Wired

Распределенный

Распределенный

Централизованный

Конвергированный доступ – основы позиционирования

Защита инвестиций на существующем оборудовании

- ❑ **Используйте конвергированный доступ**
- ❑ Заказчики, которые планируют обновление проводной + беспроводной сети
 - ❑ защита инвестиций за счет поддержки различных сервисов, доступных в будущем с ведущими коммутаторами в отрасли - Catalyst 3850, 3650 и 4K с супервизором Sup8E (Advanced QoS, AVC, UPOE)
 - ❑ линейный апгрейд (3560 -> 3650, 3750 -> 3850, Sup7E -> Sup8E)
 - ❑ внедрение беспроводной сети
 - ❑ обеспечение прозрачности трафика, расширенный QoS, максимальная надежность и масштабируемость для проводного/беспроводного доступа
- ❑ Используйте решения на AireOS или другие модели внедрения
 - ❑ Внедрения для больших кампусов
 - ❑ Необходимость развертывания ТД в режимах Flexconnect, Indoor, Outdoor Mesh или Office Extend AP (запланировано)
 - ❑ Требуется определенный функционал AireOS, не поддерживаемый IOS-XE

Instant Access – основы позиционирования

6800/6500 функциональная стабильность и операционная эффективность на уровне доступа

■ Заказчики, которые

- желают расширить на уровень доступа функционал и эксплуатационную надежность Catalyst 6500/6800
- заинтересованы в специфическом функционале Catalyst 6500/6800, как, например, MPLS, расширенное сегментирование и т.п.
- имеют блоки распределения до 1000 пользовательских портов и наложенную беспроводную сеть
- желают максимально централизовать управление сетью кампуса и/или имеют ограничения в количестве персонала
- желают упростить процедуры управления ПО на коммутаторах

■ Используйте другие модели внедрения

- существует заинтересованность заказчика в конвергированном доступе
- существует заинтересованность в сервисах, которые предоставляют интеллектуальные коммутаторы 3850/3650/sup8E на уровне доступа
- при росте потребности в сервисах mobility и application services
- системы с более чем 1000 (2000*) портов доступа в блоке распределения
- обязательна локальная коммутация

Традиционный доступ – основы позиционирования

- ЛУЧШИЕ коммутаторы на рынке (вам не надо менять дизайн сети)**
- предлагаем актуальные решения и технологии коммутации (Cat4500/Sup8E, 3850, 3650, 2960-X/XR)**
- Заказчики, которые**
 - отдают предпочтение наиболее известной модели построения проводного доступа
 - хотят использовать гибкую модель беспроводного доступа (централизованную или распределенную)
 - хотят использовать лучшие коммутаторы уровня доступа Cat 3850, 3650 & Sup8E (Advanced QoS, App Visibility, UPOE)
 - планируют линейный апгрейд (3560 -> 3650, 3750 -> 3850, Sup7E -> Sup8E)
 - имеют инфраструктуры на мультивендорных решениях проводного/беспроводного доступа
- Используйте другие модели внедрения**
 - заказчик планирует внедрение на базе конвергированного доступа
 - заказчик заинтересован в функционале Catalyst 6500/6800 и упрощении дизайна сетевой архитектуры

Ждем ваших сообщений с хештегом
#CiscoConnectRu



Спасибо

Пожалуйста, заполните анкеты

Ваше мнение очень важно для нас

Контакты:

Илья Озарнов

iozarnov@cisco.com



CiscoRu



Cisco



CiscoRussia



CiscoRu



Cisco Connect

Москва | 17–18 ноября 2015