



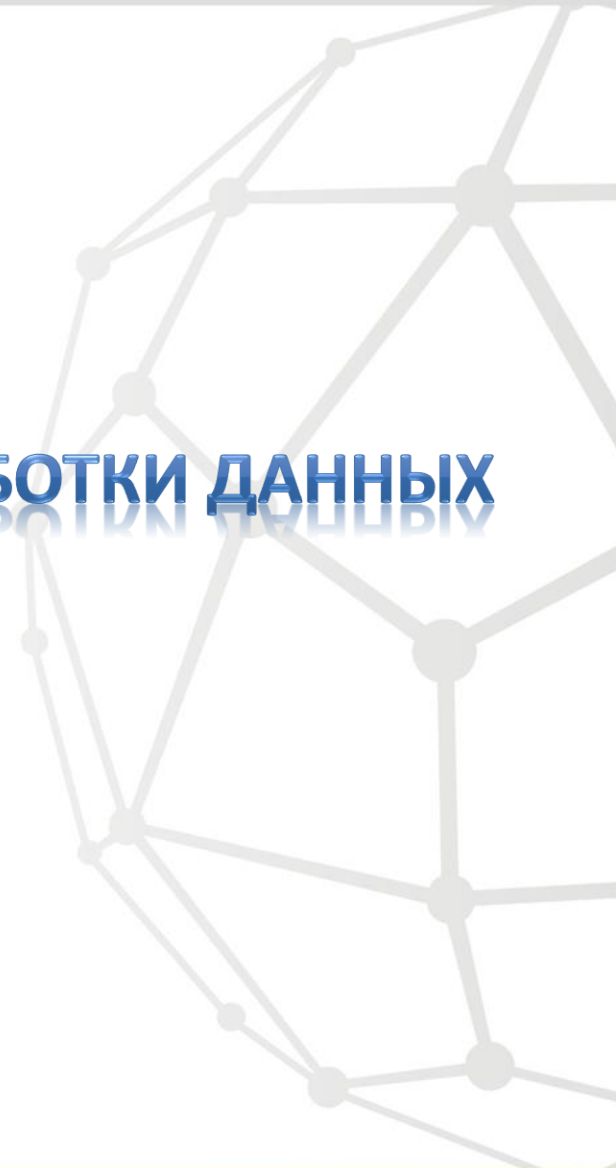
ЦЕНТР
ПРИКЛАДНЫХ
ИССЛЕДОВАНИЙ
КОМПЬЮТЕРНЫХ
СЕТЕЙ

Варианты применения ПКС

Вячеслав Васин: vvasin@arccn.ru

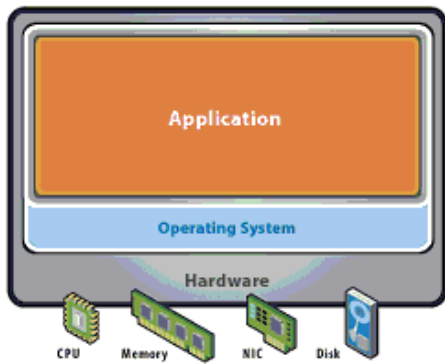


ПРИМЕНЕНИЕ ПКС В ЦЕНТРАХ ОБРАБОТКИ ДАННЫХ

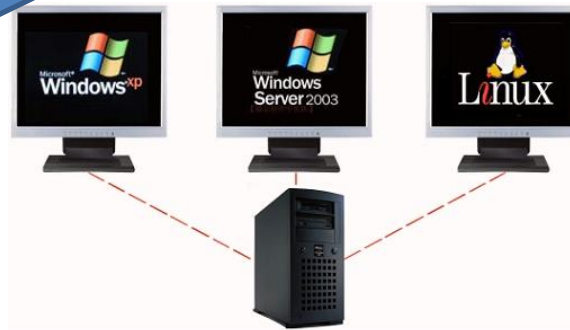
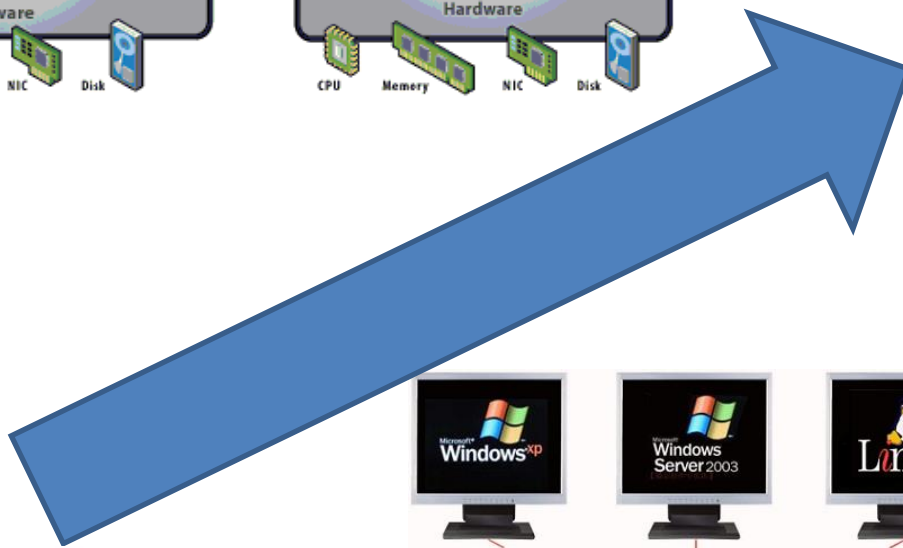
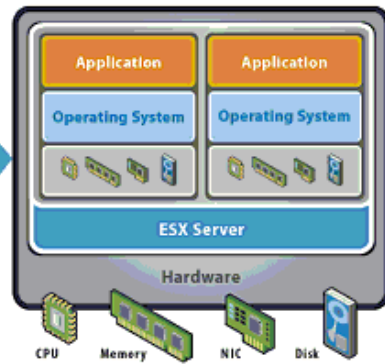


История развития ЦОД

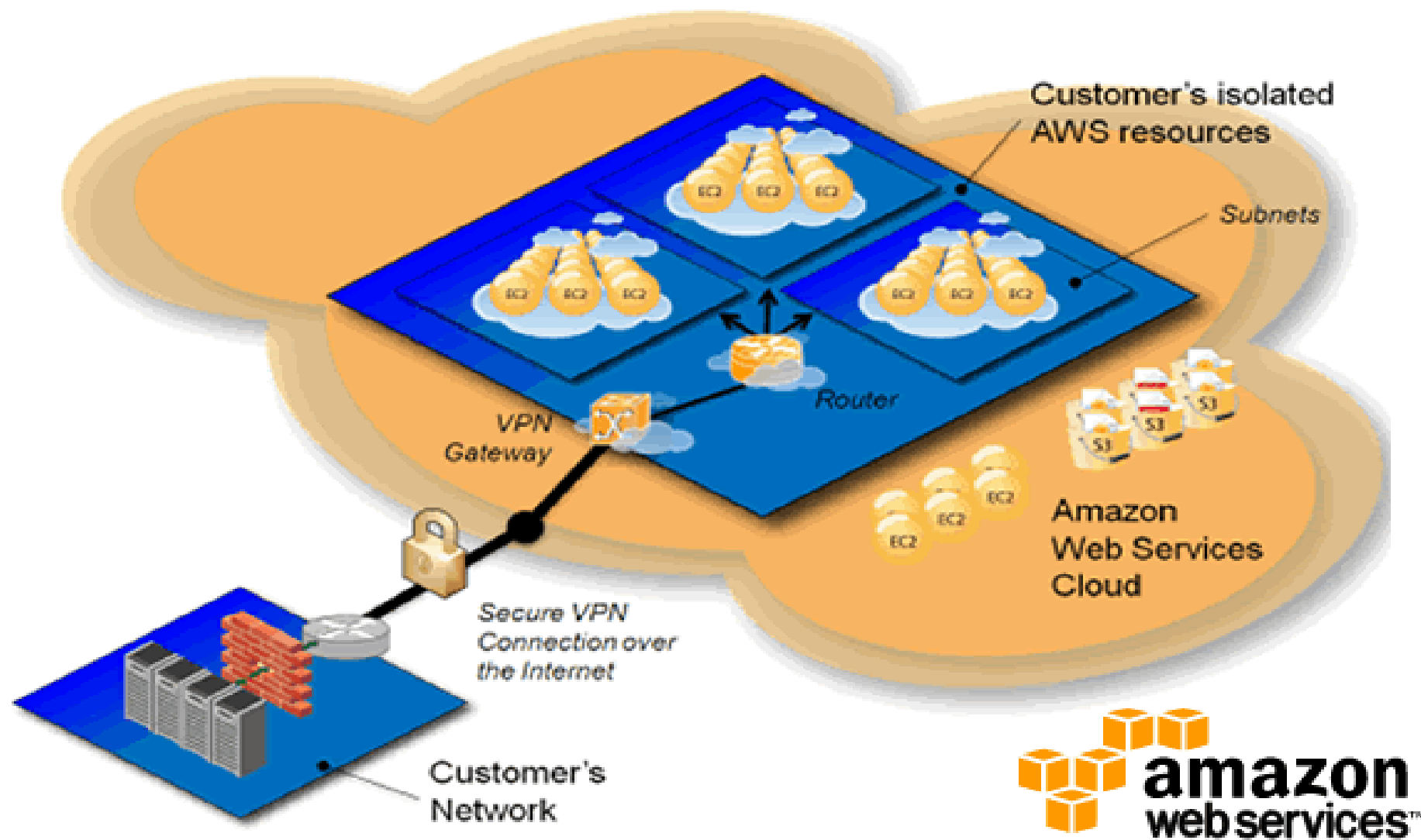
Without Virtualization



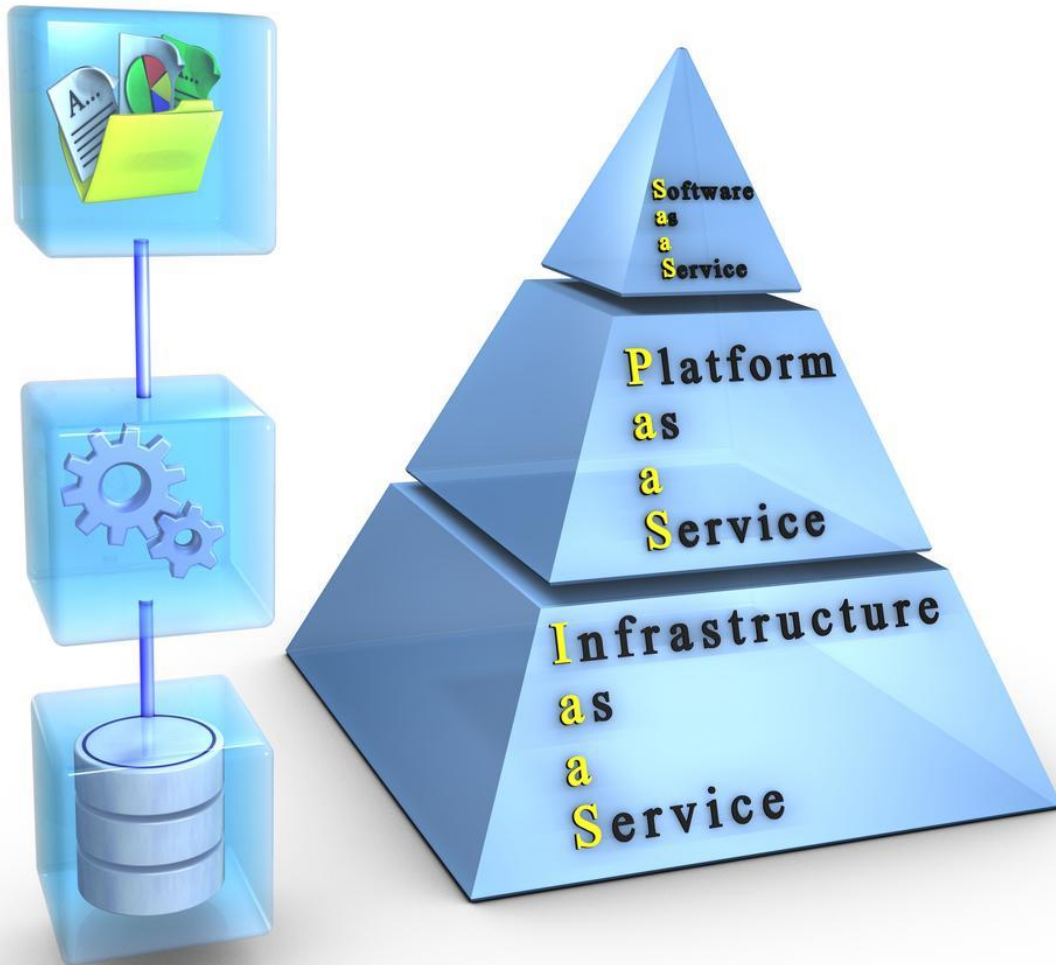
With Virtualization



Amazon Web Services - Cloud IaaS



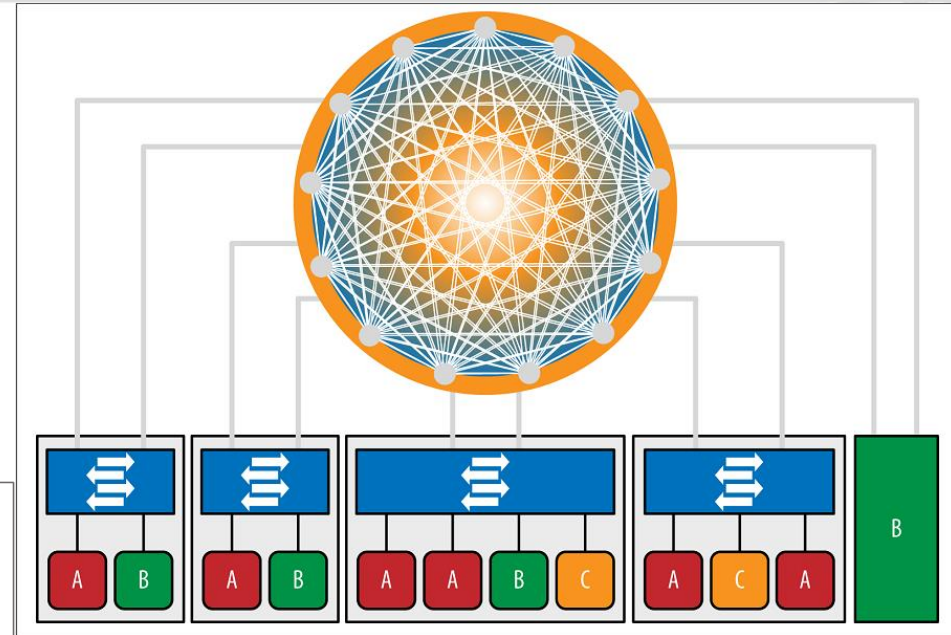
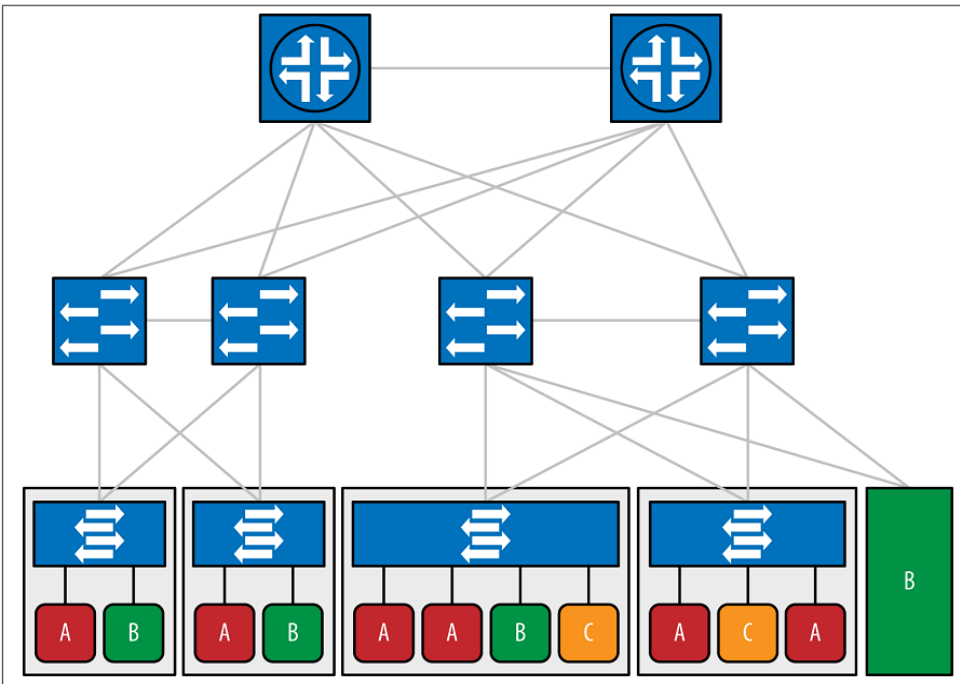
IT-as-a-Service



- SaaS - предоставление доступа к приложению. Например, база данных используемая несколькими пользователями (Salesforce).
- PaaS – предоставление доступа к среде разработки приложения (Google Apps).
- IaaS – предоставление доступа к сетевым, вычислительным ресурсам и ресурсам хранения (Amazon).

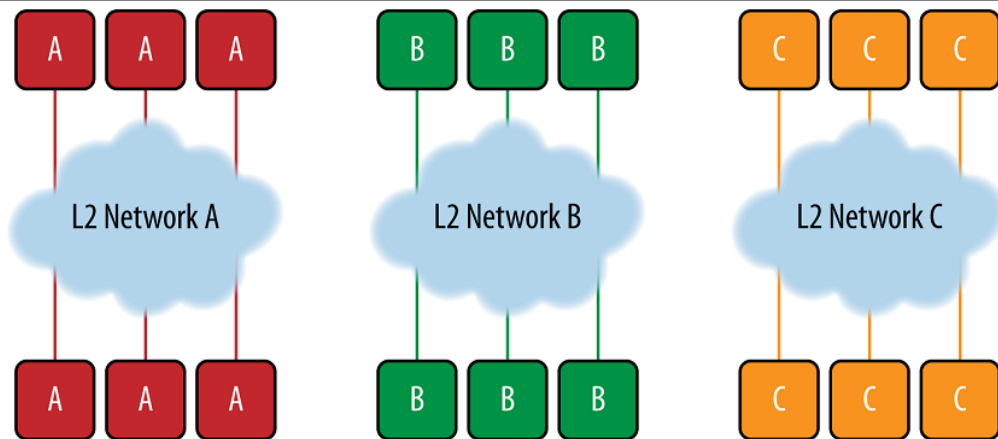
Организация связей в ЦОД

Одноуровневый дизайн ЦОД



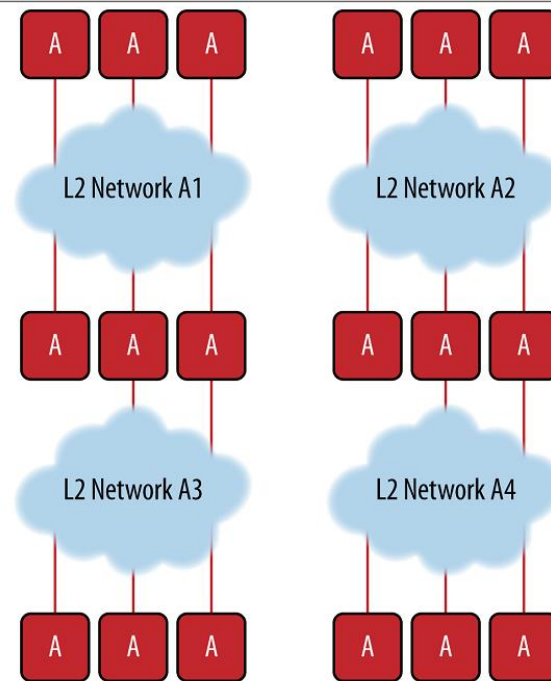
Многоуровневый дизайн ЦОД

Сетевая виртуализация в ЦОД

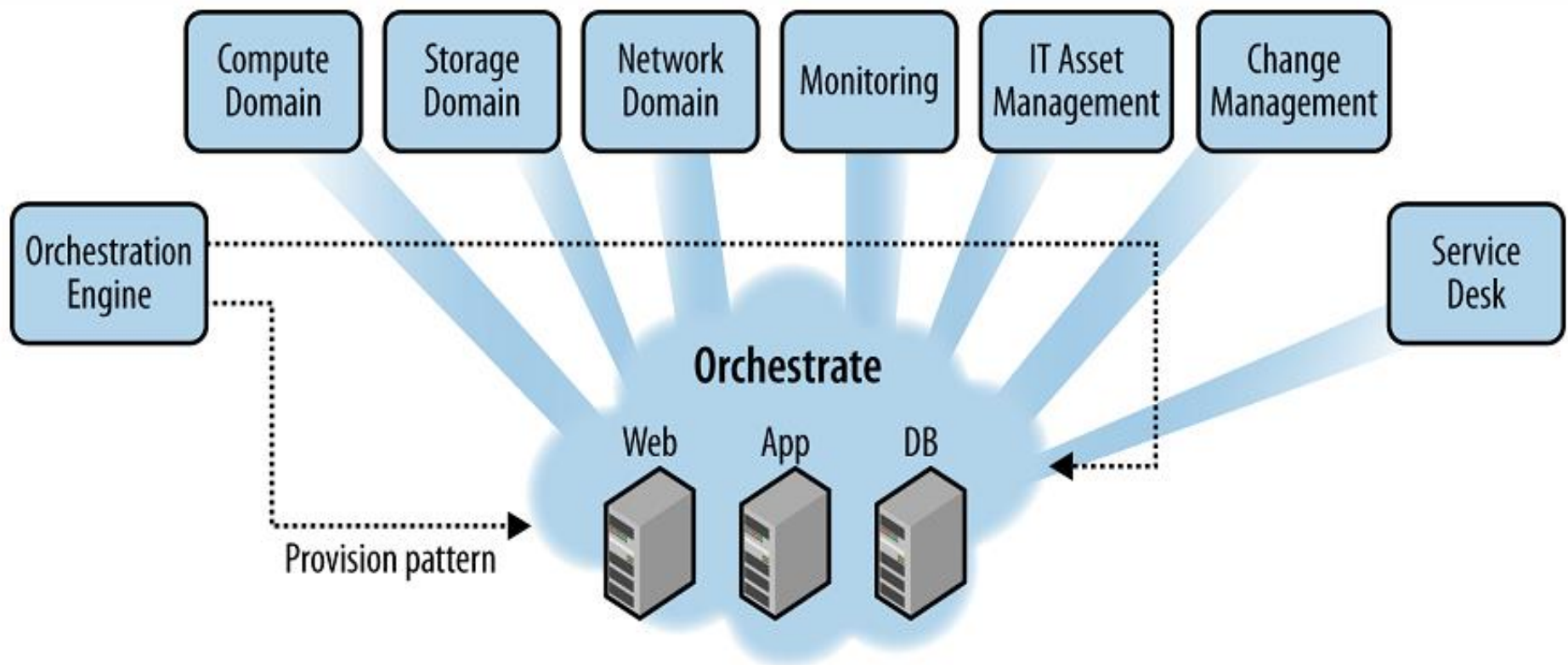


*Логическое видение сети
с точки зрения
разных заказчиков IaaS.*

*Несколько географически
распределенных сетей заказчика,
связанных между собой
различными сервис провайдерами
для организации единого сервиса,
предоставляемого клиенту.*



Управление и мониторинг ЦОД

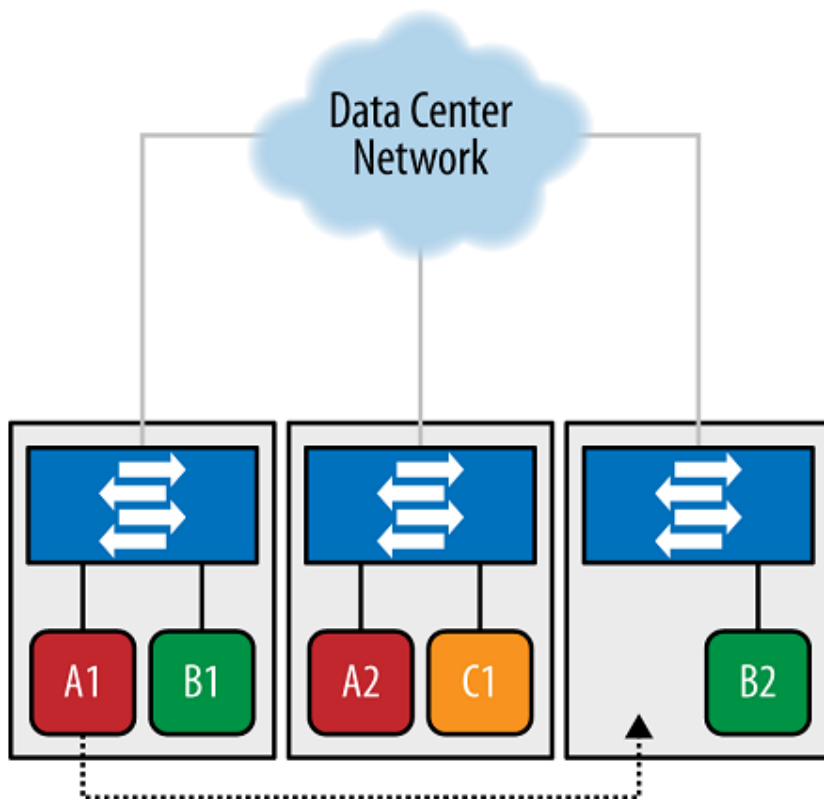


Resource Orchestration
Onboard, provision, manage
CPU, Storage and Network

Workload Orchestration
Workload aware placement,
optimization, and operation

Service Orchestration
Manage the lifecycle of
business applications

Миграция виртуальных машин:



*Восстановление
после сбоя.*

*Балансировка используемых мощностей,
в том числе потребления энергии.*

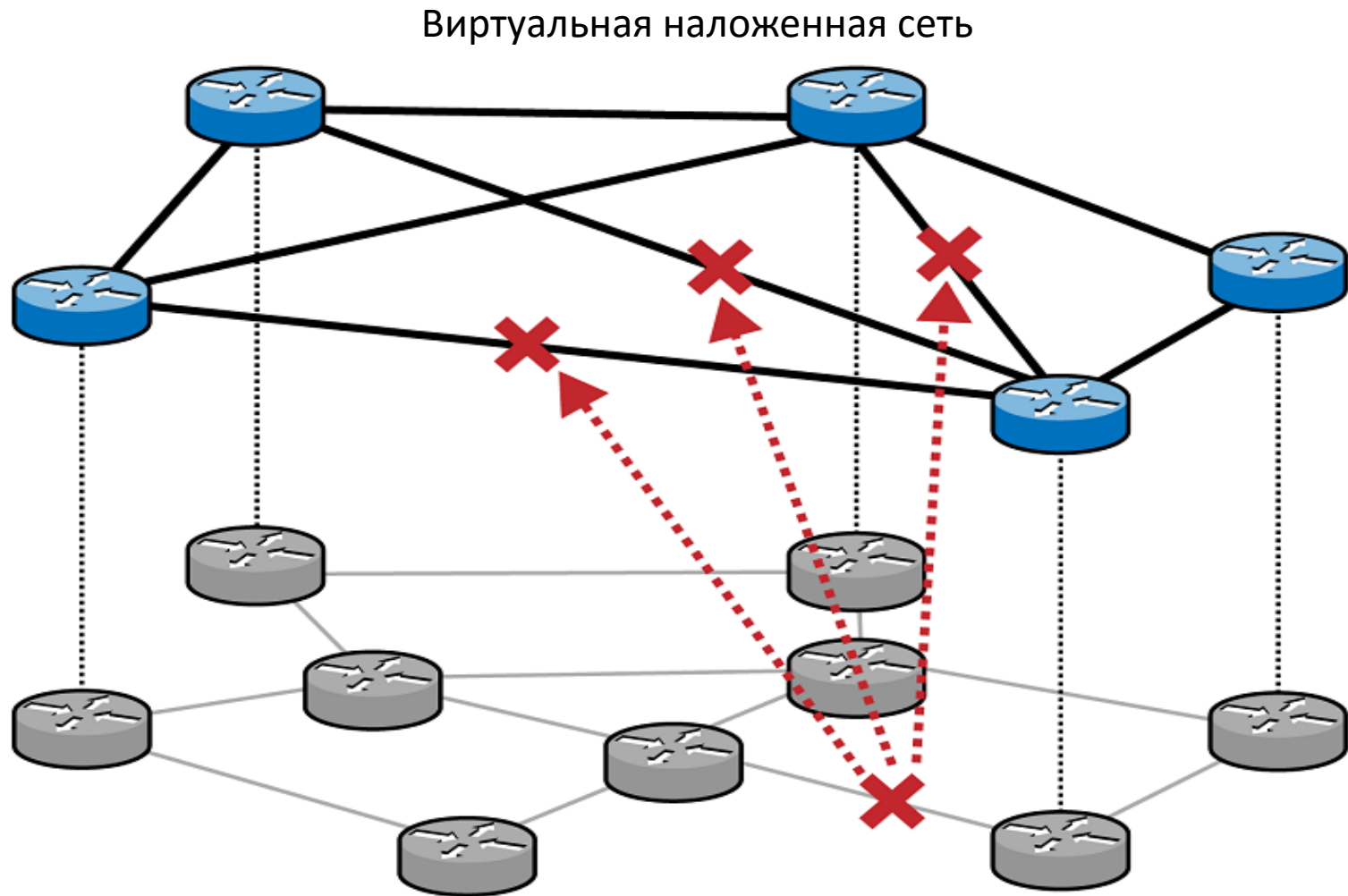
*Миграция ЦОД – объединение или
расширение.*

*Проведение сервисного
обслуживания.*

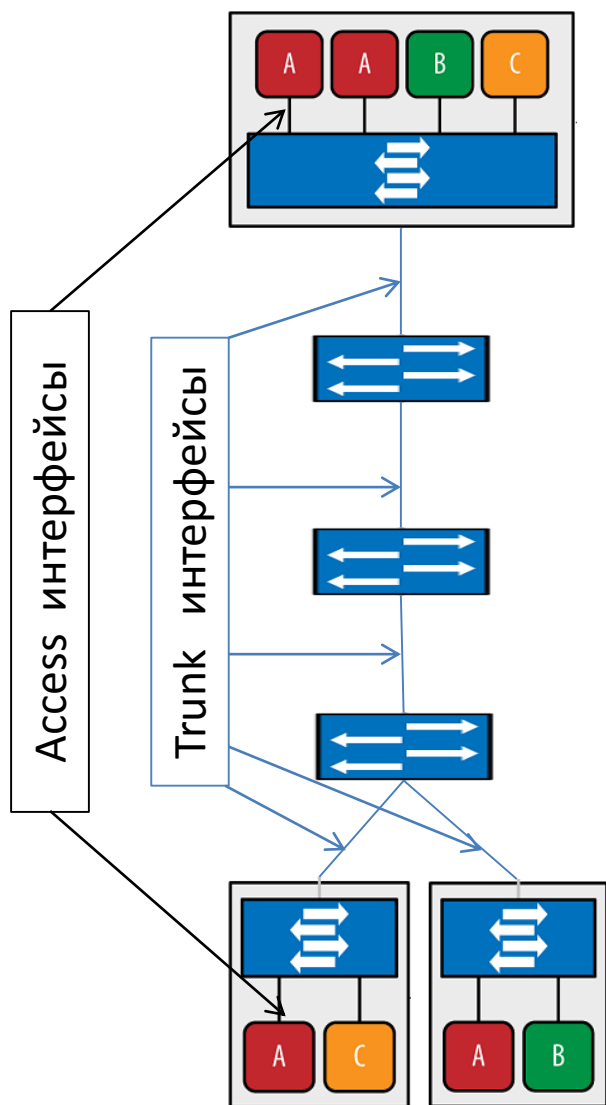
*Предотвращение
возможного сбоя.*

*Географическое перемещение ресурсов и
сервисов ближе к потребителям.*

Сетевая виртуализация



Использование VLAN в ЦОД:



*Простота в
конфигурировании.*

*Поддерживается всеми
производителями оборудования.*

*Возможность использования произвольной IP
адресации в разных VLAN.*

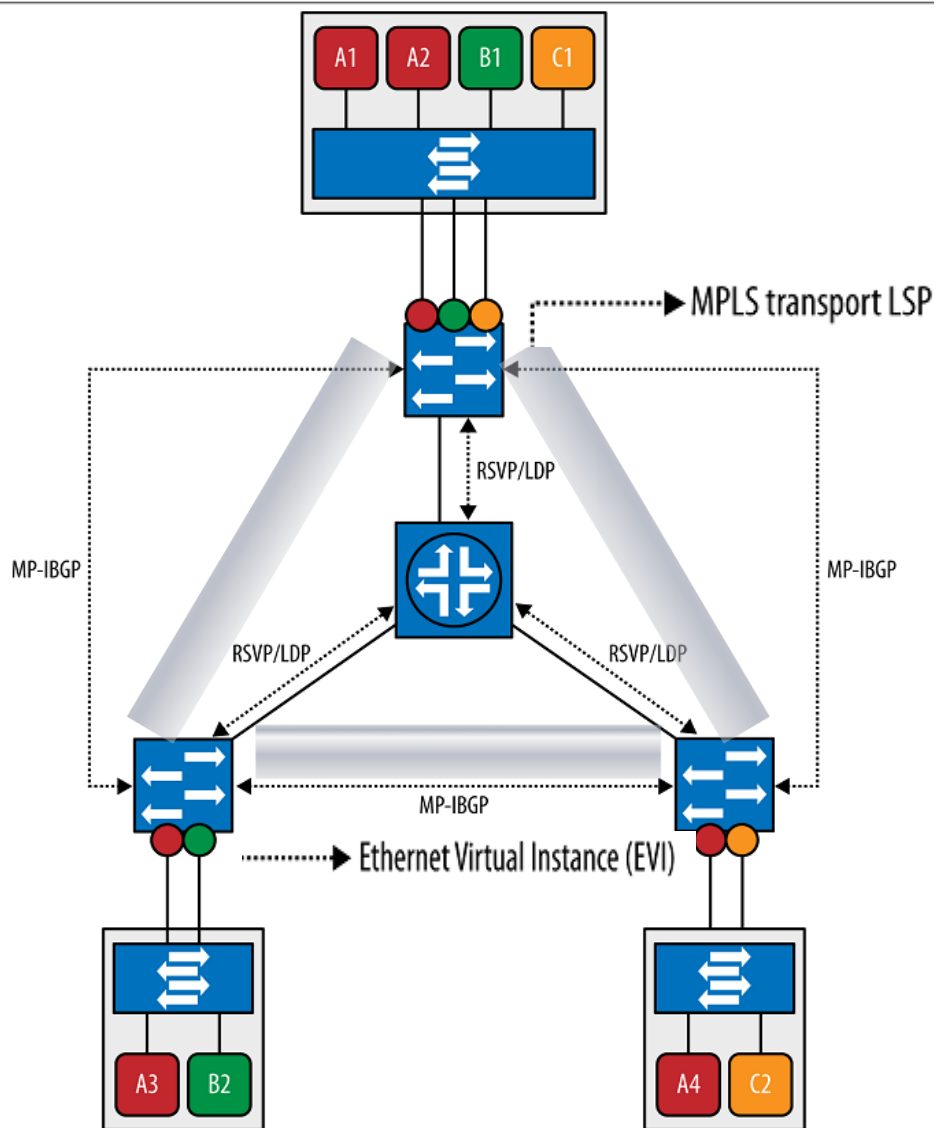
Плоская IP сеть.

*Ограничено общее
количество VLAN.*

*Медленное перестроение
сети в случае сбоя.*

*Не поддерживается
балансировка нагрузки.*

Использование Ethernet VPN в ЦОД:



Масштабирование за пределы ограничения в 4094 VLAN.

Масштабируемость на большое количество устройств.

Упрощение конфигурирования и мониторинга при поддержке XMPP.

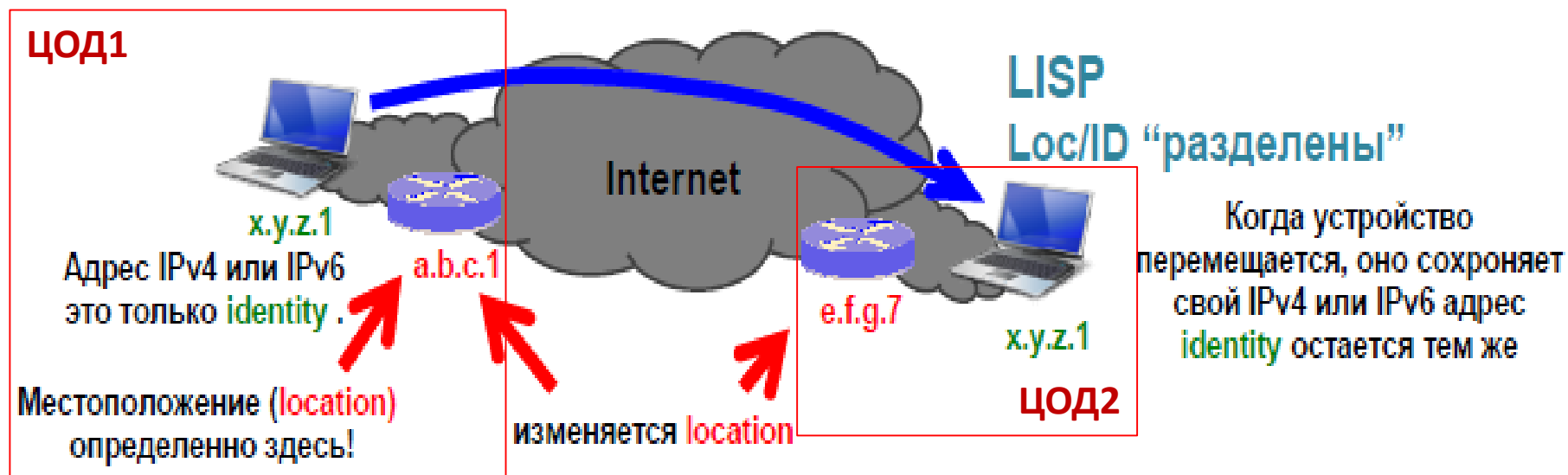
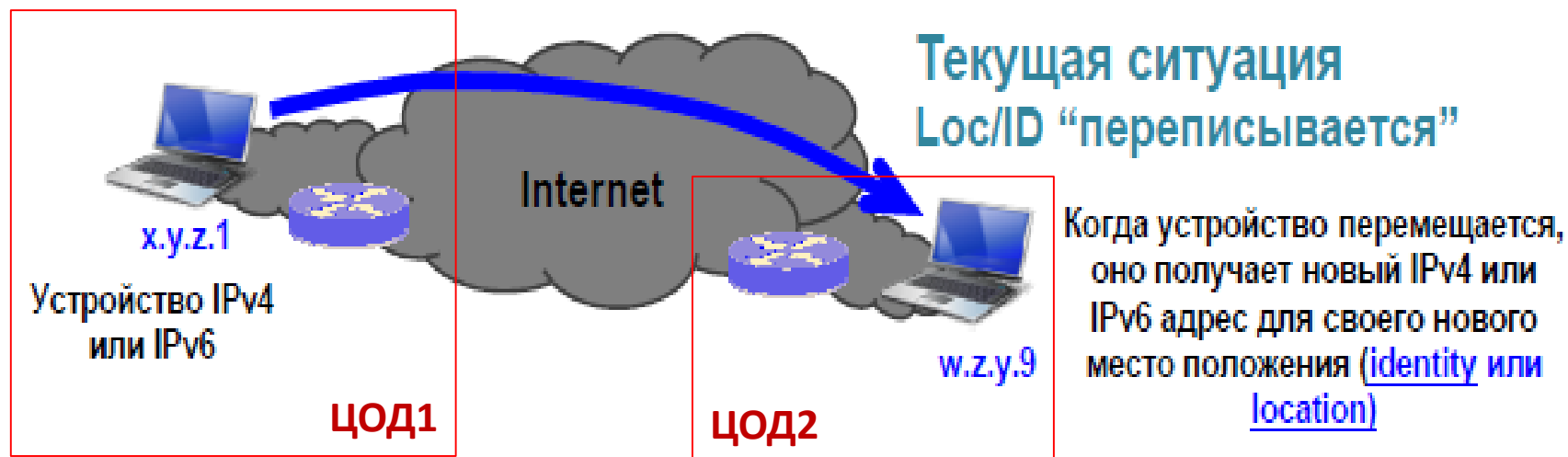
Меньшее количество туннелей по сравнению с VxLAN и NVGRE.

Сложный поиск неисправностей при использовании множества протоколов.

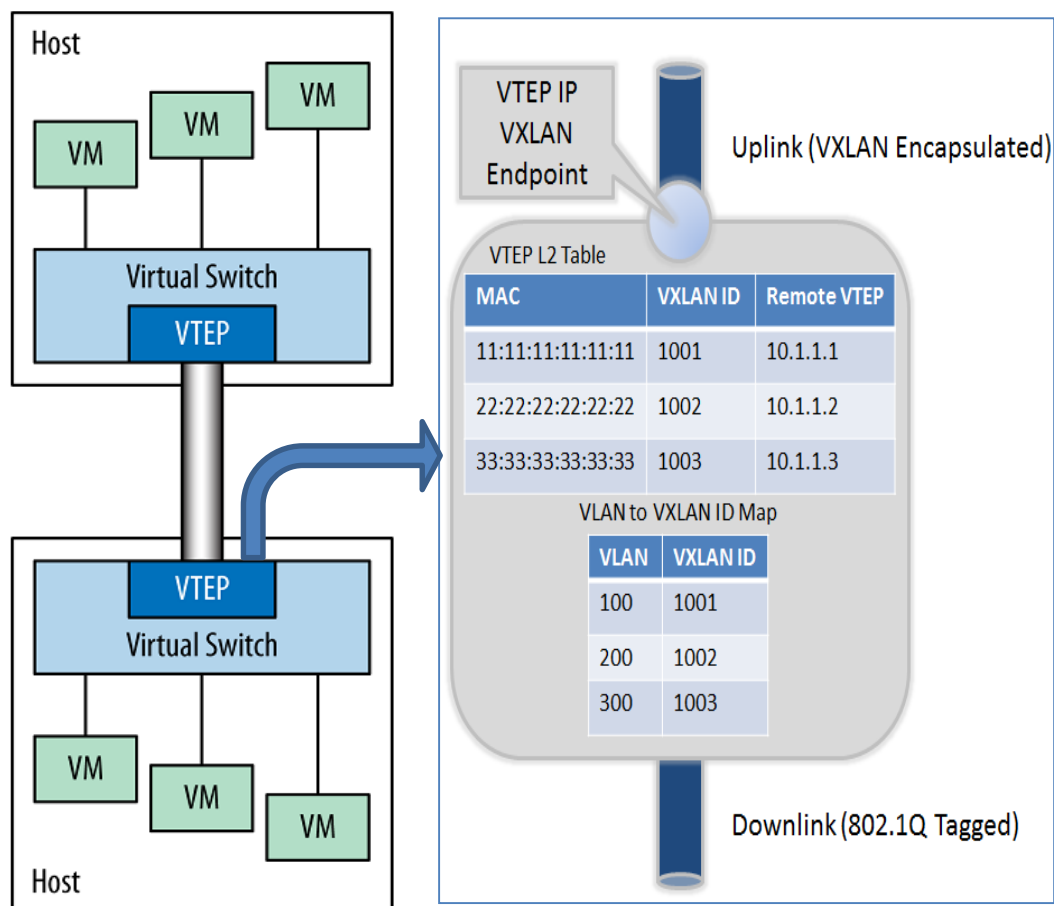
Более сложное конфигурирование устройств.

Необходимость аппаратной поддержки MPLS в оборудовании ЦОД.

Locator/ID Separation Protocol (LISP)



Virtual Extensible Local Area Network (VXLAN):



Outer MAC DA	Outer MAC SA	Outer 802.1Q	Outer IP DA	Outer IP SA	Outer UDP	VXLAN ID (24 bits)	Inner MAC DA	Inner MAC SA	Optional Inner 802.1Q	Original Ethernet Payload	CRC
--------------	--------------	--------------	-------------	-------------	-----------	--------------------	--------------	--------------	-----------------------	---------------------------	-----

VxLAN инкапсуляция

Исходный фрейм

Поддержка L2 unknown unicast, broadcast.

Поддержка свыше 16 миллионов сущностей.

Работает поверх L3 доменов.

Стандартизуется IETF.

Внешние коммутаторы не видят VM-IP и VM-MAC.

VM не видит VxLAN.

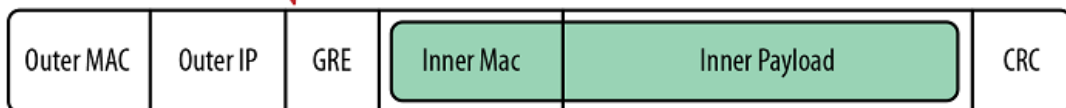
Дополнительные издержки (50 байт) на заголовок.

Сложность конфигурирования.

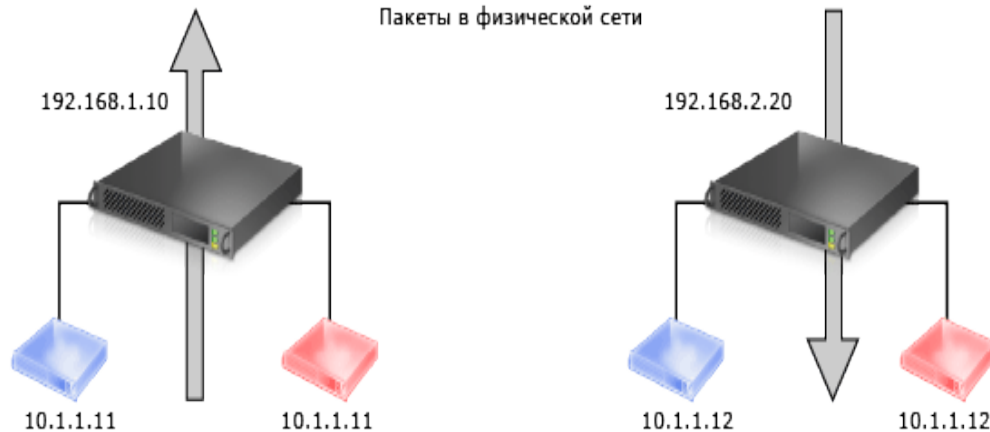
Необходимость поддержки VxLAN оборудованием ЦОД.

Network Virtualization using Generic Routing Encapsulation (NVGRE):

TNI → 24-bit ID Tenant Network Identifier



Пакеты в физической сети



Поддержка свыше 16 миллионов сущностей.

Поддержка стандартного протокола – GRE.

Работает поверх L3 доменов.

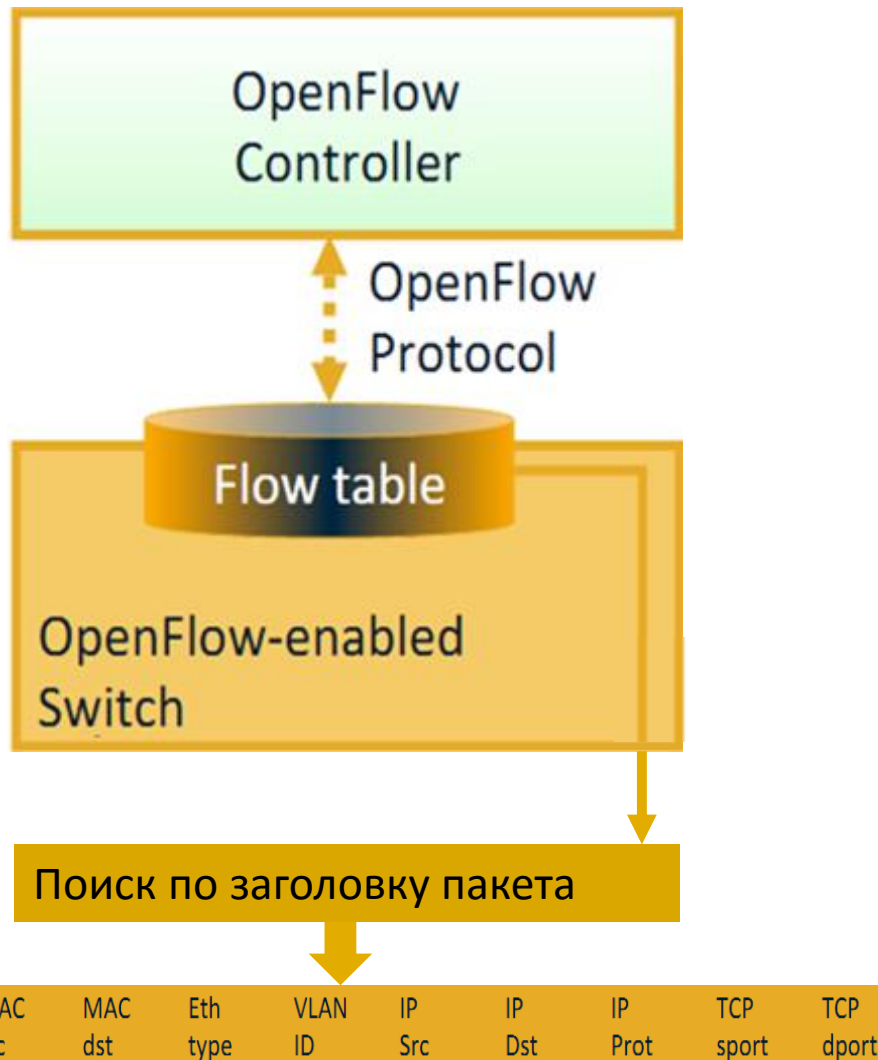
Поддержка GRE производителями оборудования.

Отсутствие UDP не позволяет делать балансировку по потокам.

Дополнительные издержки (46 байт) на заголовок.

Сложность конфигурирования.

OpenFlow:



Детальный контроль потоков.

Гибкость в реализации политик.

Тонкая настройка механизмов балансировки нагрузки.

Организация виртуализации без издержек на доп. Заголовки.

Централизованное управление и мониторинг.

Необходимость поддержки OpenFlow коммутаторами ЦОД.

Типы наложенных сетей

L2 Overlay

- GRE (32 bit GRE key);
- VxLAN (24 bit VxLAN Network Identifier);
- NVGRE (24 bit Virtual Subnet ID);
- Vmware/Nicira (64 bit Context ID);
- MPLS (20 bit Label)

L3 Overlay

- L3 MPLS VPN

Hybrid overlay-underlay

- Plexxi

Software Defined Data Center

Плюсы

Оптимизация управления инфраструктурой ЦОД

Уменьшение зависимости от аппаратуры

Автоматизация выполняемых задач

Масштабируемость, эффективность, гибкость

Быстрота реализации требуемого функционала

Минусы

Разнородность решений разных производителей

Отсутствие зрелых стандартов

Сырость предлагаемых решений

Недостаточный набор реализованных функций

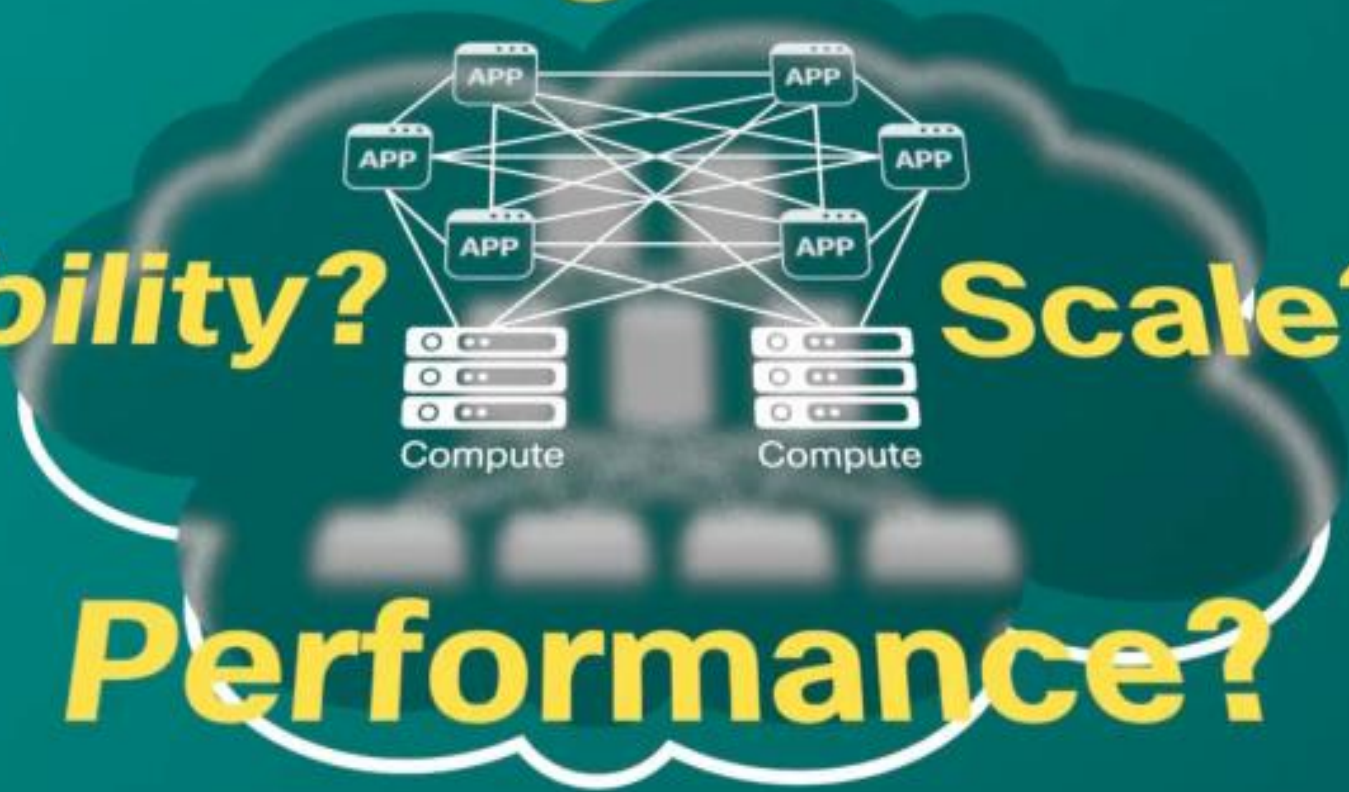
Требования приложений к ЦОД:

Management?

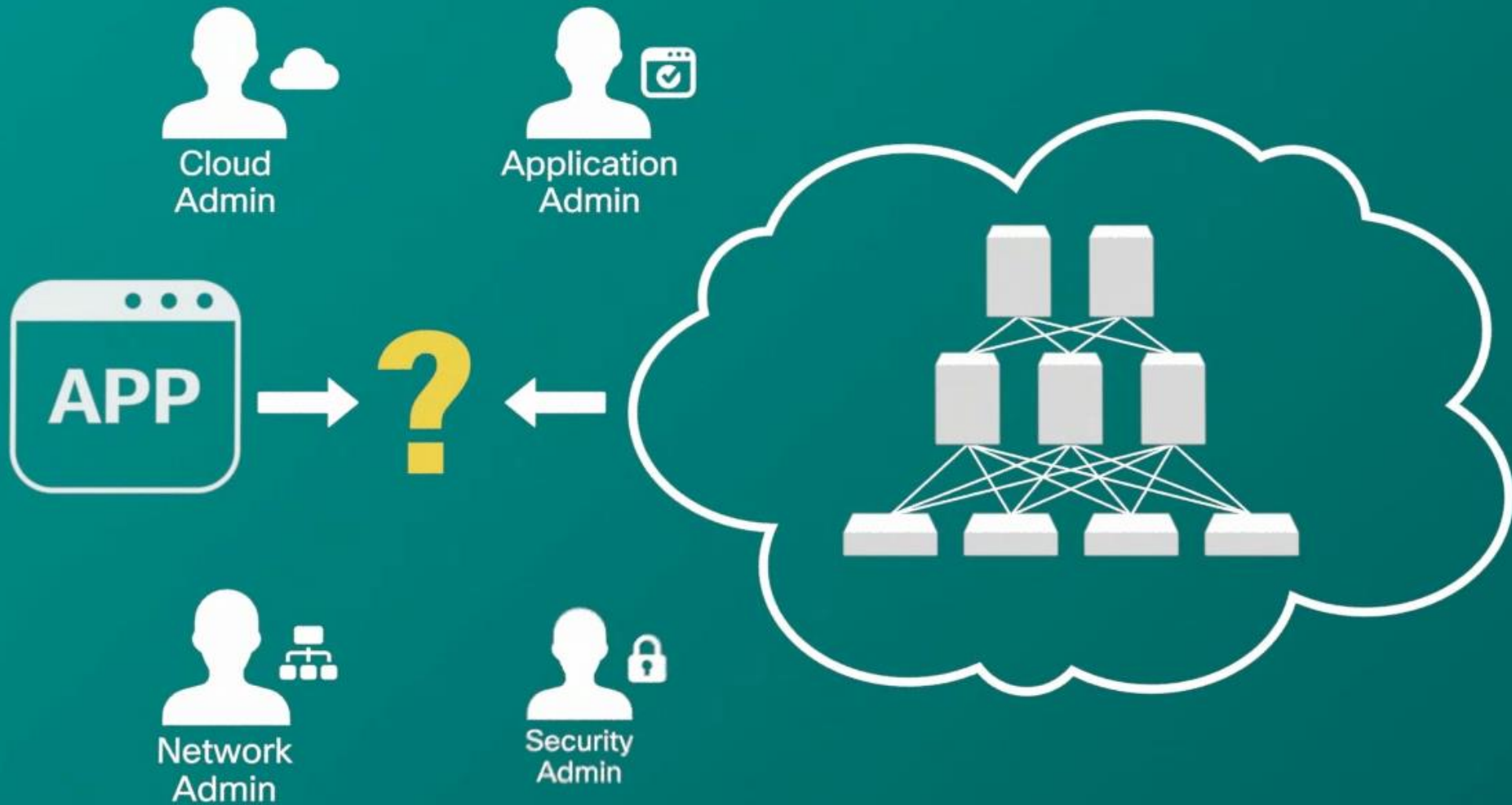
Visibility?

Scale?

Performance?

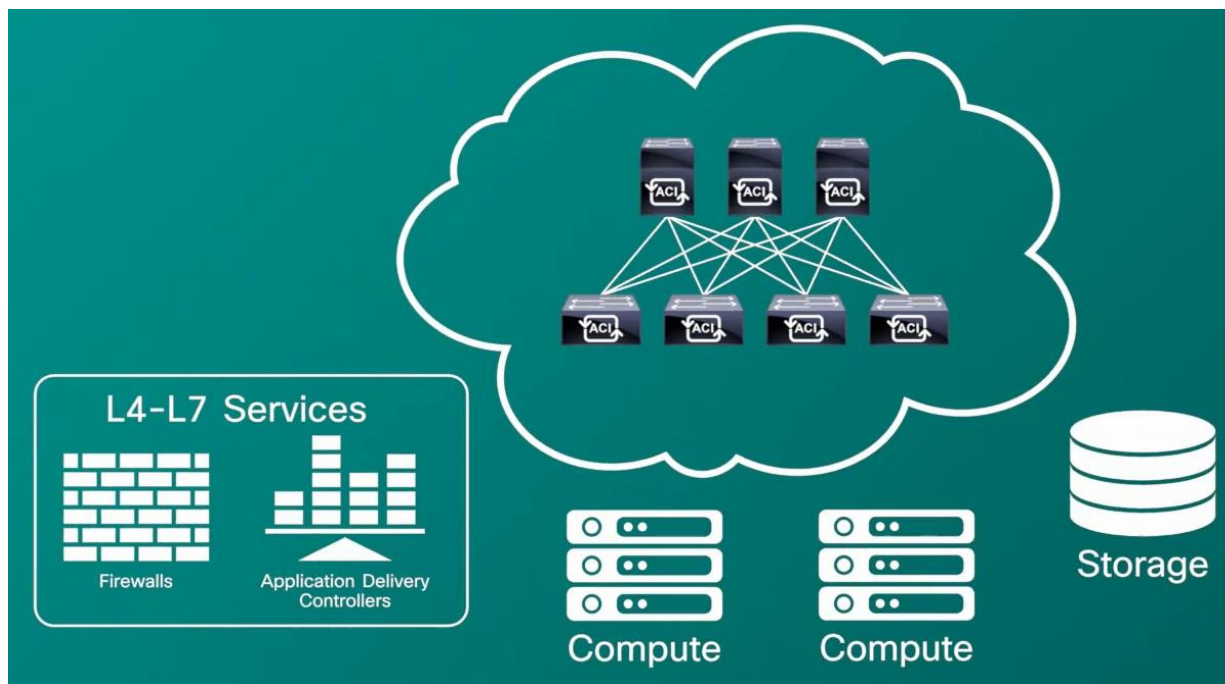


Текущие проблемы эксплуатации облачных сервисов:



Cisco Application Centric Infrastructure (ACI):

Новая модель построения ЦОД:

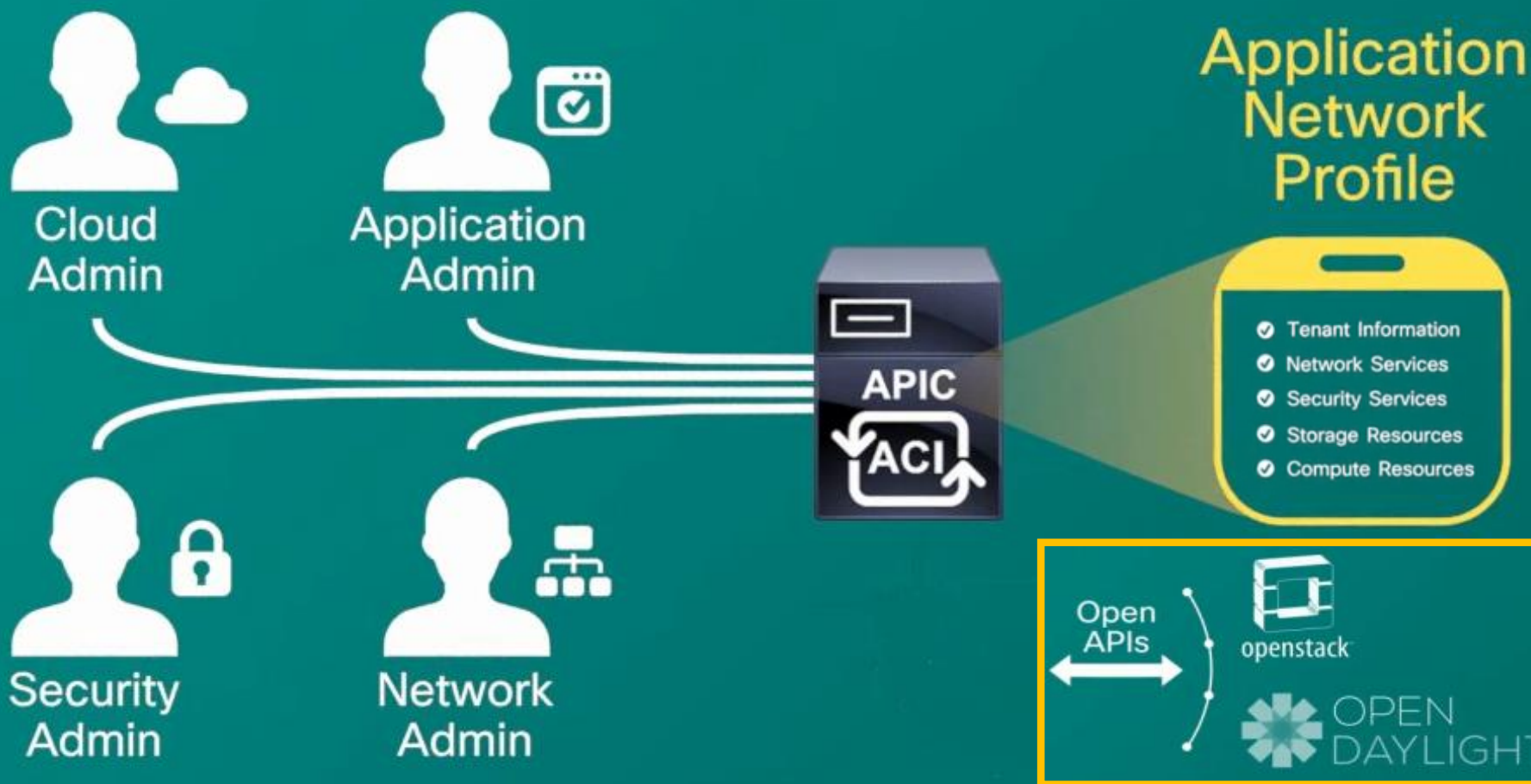


- Ориентация на приложения.
- Автоматизация и унификация физической и виртуальной инфраструктуры.
- Мониторинг работы всей инфраструктуры в реальном времени.
- Беспрецедентная производительность и масштабируемость.
- Ускорение реализации приложений.

Application Policy Infrastructure Controller (APIC)

Контроллер инфраструктуры политик приложений.

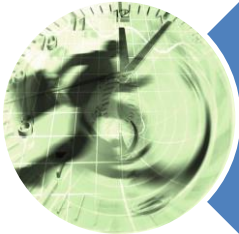
Единая точка автоматизации и управления для матричной структуры Cisco ACI.



АСІ обеспечивает:



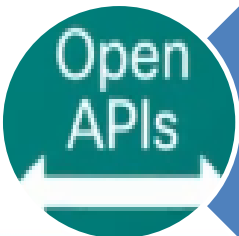
75-процентное сокращение совокупной стоимости владения



Сокращение сроков внедрения приложений до нескольких минут



Централизацию управления политиками, упрощение текущей работы и расширение возможности ИТ-специалистов



Небывало высокий уровень защиты инвестиций специалистов достигается с помощью открытых протоколов, интерфейсов API и стандартов

Коммутаторы Nexus 9000 обеспечивают:

Гибкость и простота

- Разделение политик, ориентированных на приложения и IP-инфраструктуры.
- Динамическое согласование физических и виртуальных сетевых сервисов.

Производительность и масштабируемость

- Скорости 10/40 в будущем 100 Гбит/с. 55 тысяч портов 10G.
- Емкость коммутации составляет 60 Тбит/с. 1 миллион конечных устройств.

Информационная безопасность

- Централизованные программируемые политики.
- Новые решения Cisco ASAv.

Прозрачность и диагностика в реальном времени

- Статистическая, диагностическая информация по арендатору, приложению.
- Аналитика, возможность мониторинга и изоляции случаев потери пакетов.

Открытость платформ и исходных кодов

- Интерфейсы RESTful API.
- Open Source [OpenStack, Open Daylight, виртуальные коммутаторы и VXLAN].

Широкая поддержка виртуализации

- Microsoft Hyper-V, RedHat KVM, VMware vSphere.
- Виртуальный коммутатор Cisco Application Virtual Switch (AVS).

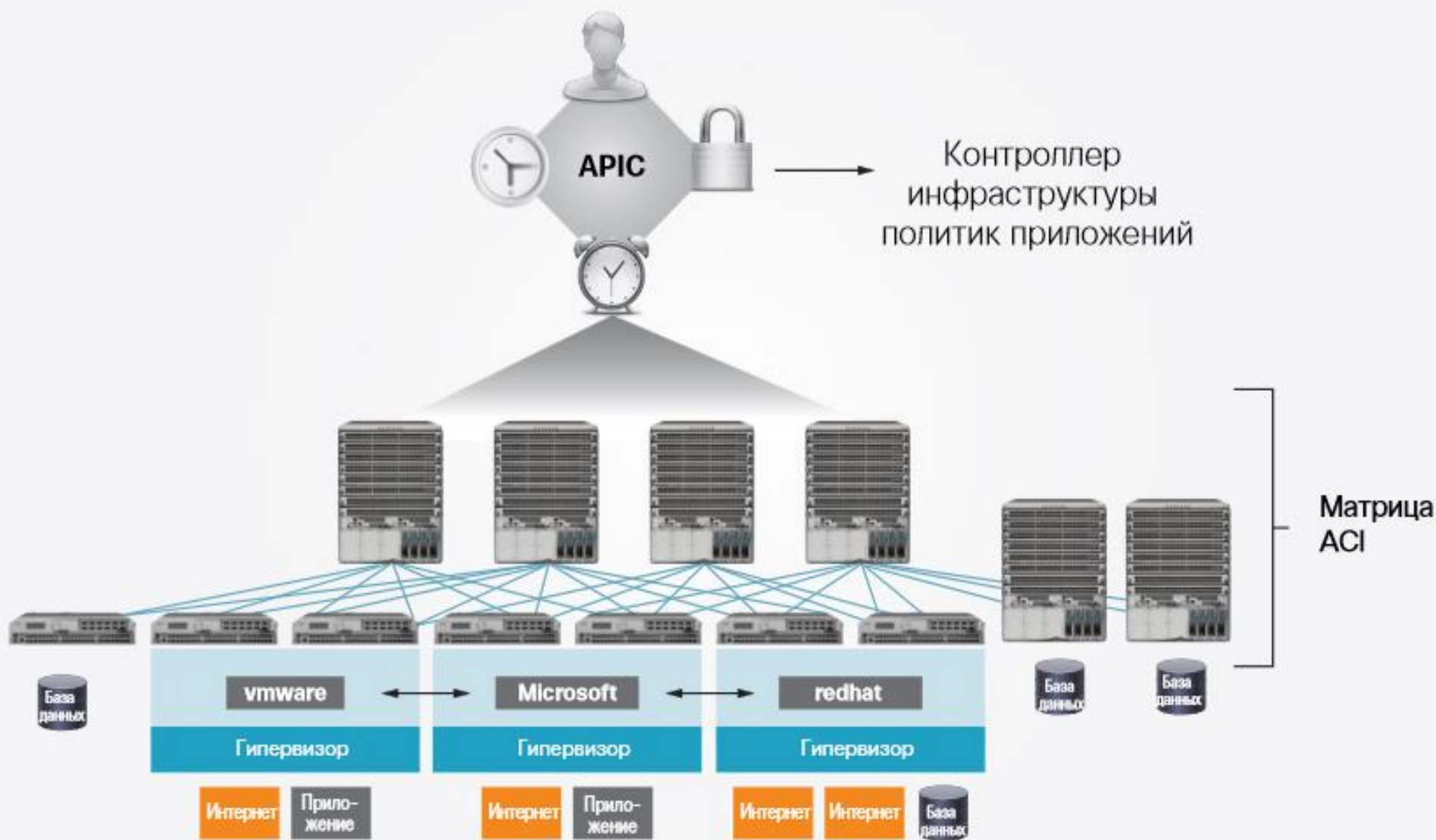
Современные возможности программируемости

- Взаимодействие с группами разработчиков за счет интерфейсов RESTful API.
- Средства скриптования Puppet, Chef, CFEngine, Python и другие инструменты.

Системные инновации

- Коммутатор ЦОД без коммутационной панели с поддержкой портов 100G.
- 15-процентное повышение эффективности энергопотребления и охлаждения.

Инфраструктура Cisco ACI:



Преимущества новой архитектуры для разных потребителей:

Пользователи

Владельцы приложений
и бизнес-подразделений

Преимущества

Значительное сокращение
времени, необходимого
для предоставления
сервисов

Повышение
предсказуемости затрат
на приложения и ИТ

Комплексная оценка
работоспособности
приложения, которая
помогает соблюдать SLA

Эффект

Своевременное
развертывание
приложений

Оптимизированная
структура расходов

Повышение доступности

Преимущества новой архитектуры для разных потребителей:

Пользователи

Группы управления:
серверами, системами
хранения данных и
виртуализацией

Преимущества

Центральная модель
развертывания ускоряет
настройку сети и
инфраструктуры
безопасности

Помощь в реализации
модели развертывания
любого уровня нагрузки
в любом месте

Эффект

Эксплуатационная
эффективность

Быстрое развертывание

Повышение доступности
и повышение уровня
удовлетворенности
заказчиков

Преимущества новой архитектуры для разных потребителей:

Пользователи

Группа управления сетью

Преимущества

Автоматизированное выделение сетевых ресурсов снижает накладные расходы, сокращает количество ошибок, ускоряет развертывание

Автоматизированное устранение неполадок, а так же контроль физической и виртуальной инфраструктур сокращают среднее время решения проблемы (MTTR)

Корреляция показателей физической и виртуальной инфраструктур в режиме реального времени

Эффект

Повышение производительности, точности и упрощение масштабирования

Повышение доступности

Повышение уровня удовлетворенности заказчиков

Преимущества новой архитектуры для разных потребителей:

Пользователи

Группа управления
безопасностью

Преимущества

Автоматизация применения
политик безопасности с
сохранением контроля над
политиками для
соответствия нормативным
требованиям

Автоматизированная
вставка виртуальных служб
обеспечения безопасности
упрощает развертывание
приложений

Эффект

Повышение уровня
безопасности и более
быстрое выделение
ресурсов

Упрощение эксплуатации

Преимущества новой архитектуры для разных потребителей:

Пользователи

Группа управления
облачными сервисами

Преимущества

АСИ повышает
согласованность политик
и сервисов для локальных
и облачных приложений

Отсутствие зависимости
от базовой
инфраструктуры
упрощает развертывание
приложений, миграцию и
управление ими

Эффект

Согласованность и
адаптивность всей
инфраструктуры

Гибкое развертывание,
более удобное
масштабирование и
снижение совокупной
стоимости владения

Преимущества архитектуры в зависимости от модели развертывания:

Модели развертывания

Центр обработки
данных с широкими
возможностями
масштабирования

Преимущества

Возможность
программирования с
использованием всех
популярных наборов
инструментов

Возможность масштабирования:

1. поддержка 10 и 40 Гбит/с
2. 1000000 IP и 64000 пользователей
3. аппаратная маршрутизация и шлюзы в сети VXLAN

Дистанционное измерение
показателей сети для
контроля
работоспособности
приложений

Эффект

Гибкость, управление и
настройка

Многопользовательская
среда с широкими
возможностями
масштабирования

Более быстрое
устранение неполадок

Преимущества архитектуры в зависимости от модели развертывания:

Модели развертывания

Поставщики услуг и
облачные центры
обработки данных

Преимущества

Крупномасштабная
многопользовательская
среда и обеспечение
безопасности приложений
на аппаратном уровне

Улучшенные показатели
матрицы коммутации и
оценка состояния для
приложений, заказчиков и
инфраструктуры

Автоматизированное
предоставление доступа к
приложениям, сетевым
сервисам и средствам
безопасности

Эффект

Безопасная
многопользовательская
среда

Упреждающее
устранение неполадок

Упрощение
эксплуатации

Преимущества архитектуры в зависимости от модели развертывания:

Модели развертывания

Предприятие

Преимущества

Готовое решение для
создания частного облака
со средствами контроля,
устранения неполадок и
обеспечения
мобильности для
приложений

Помощь в соблюдении
соглашений об уровне
обслуживания и
требований к
производительности

Эффект

Своевременное
развертывание
приложений