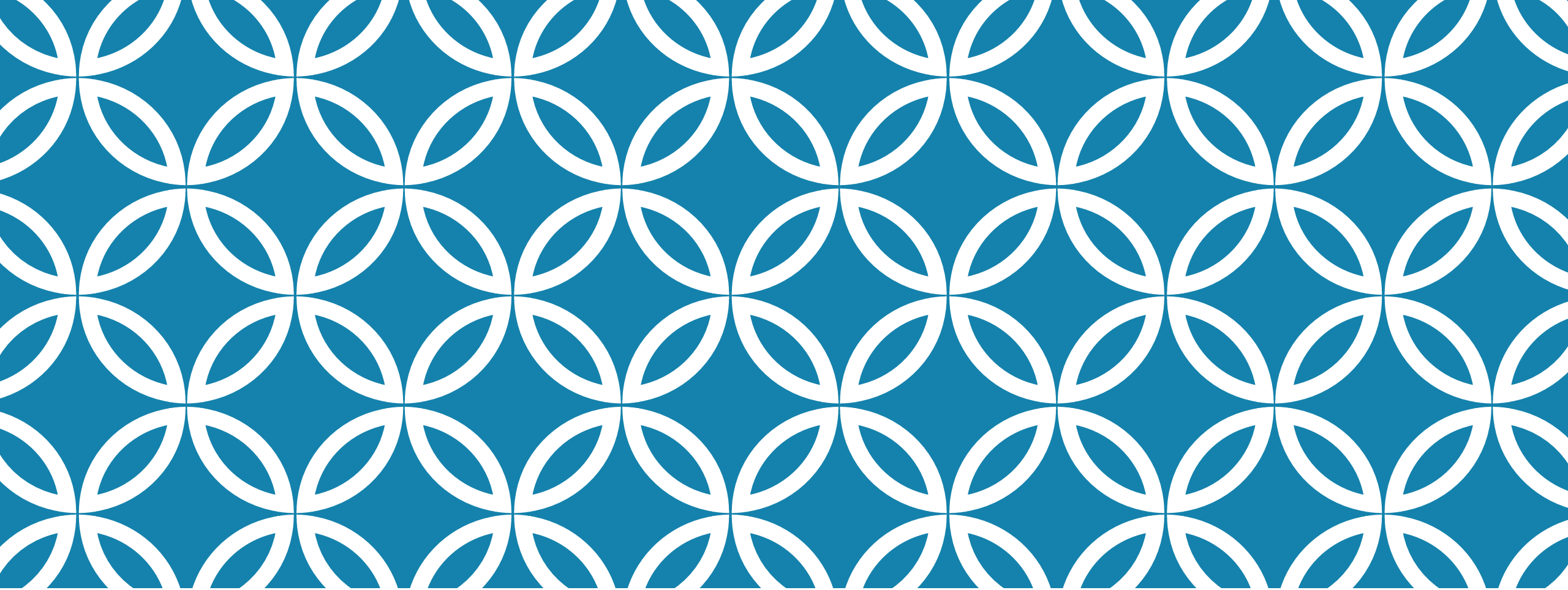


МОДУЛЬ 13. ВИРТУАЛИЗАЦИЯ СЕТИ

КАФЕДРА ТЕЛЕКОММУНИКАЦИЙ

13.1 ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ
13.1.1 ОБЗОР ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Облачные вычисления решают различные проблемы управления данными:

- повсеместный доступ к данным организации в любое время;

- оптимизацию ИТ-инфраструктуры в организации за счет подписки только на необходимые сервисы;

- исключение или снижение необходимости развертывания и поддержки оборудования на площадках;

- сокращение затрат на оборудование и электроэнергию, уменьшение требований к материальной части и потребности в обучении персонала;

- оперативное реагирование на растущие требования к объему данных.

13.1.2 ОБЛАЧНЫЕ УСЛУГИ

Три основных типа услуг облачных вычислений, согласно определению Национального института по стандартам и технологиям (США) из особой публикации 800-145, следующие:

ПО как услуга (SaaS). Поставщик облачных сервисов отвечает за доступ к приложениям и услугам, предоставляемым через Интернет.

Платформа как услуга (PaaS). Поставщик облачных сервисов отвечает за доступ к средствам разработки и сервисам, используемым для предоставления приложений.

Инфраструктура как услуга (IaaS). Облачный поставщик отвечает за предоставление ИТ-менеджерам доступа к сетевому оборудованию, виртуализированным сетевым сервисам и поддержке сетевой инфраструктуры.

Поставщики облачных сервисов расширили эту модель, включив ИТ-поддержку для каждого из облачных сервисов (ИТ как услуга, ITaaS). Для предприятий модель ITaaS может расширить возможности сети без инвестиций в новую инфраструктуру, обучения нового персонала или лицензирований нового программного обеспечения.

13.1.3 МОДЕЛИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Четыре основные модели развертывания облака:

Общедоступные облака. Приложения и услуги доступны неограниченному кругу лиц.

Частные облака. Приложения и службы предназначены для конкретной организации или структуры, например правительственной организации.

Гибридные облака. Гибридные облака состоят из двух или более облаков (например, частного и общедоступного), причем каждая из частей остается отдельным объектом, но они связаны между собой в рамках единой архитектуры.

Среды распределенных сетевых вычислений сообщества. Они создаются для исключительного использования определенным сообществом. Различия между общедоступным облаком и коллективным облаком заключаются в функциональных потребностях, настроенных для сообщества. Например, медицинские учреждения должны соблюдать политики и законы (например, HIPAA, закон об ответственности и переносе данных о страховании здоровья граждан), которые требуют особой аутентификации и конфиденциальности.

13.1.4 ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ И ЦЕНТР ОБРАБОТКИ ДАННЫХ

Далее приведены определения центра обработки данных и облачных вычислений.

Центр обработки данных. Обычно это специализированная система для хранения и обработки данных, принадлежащая ИТ-отделу компании или арендуемая у третьих сторон. ЦОД обычно дорого создавать и обслуживать.

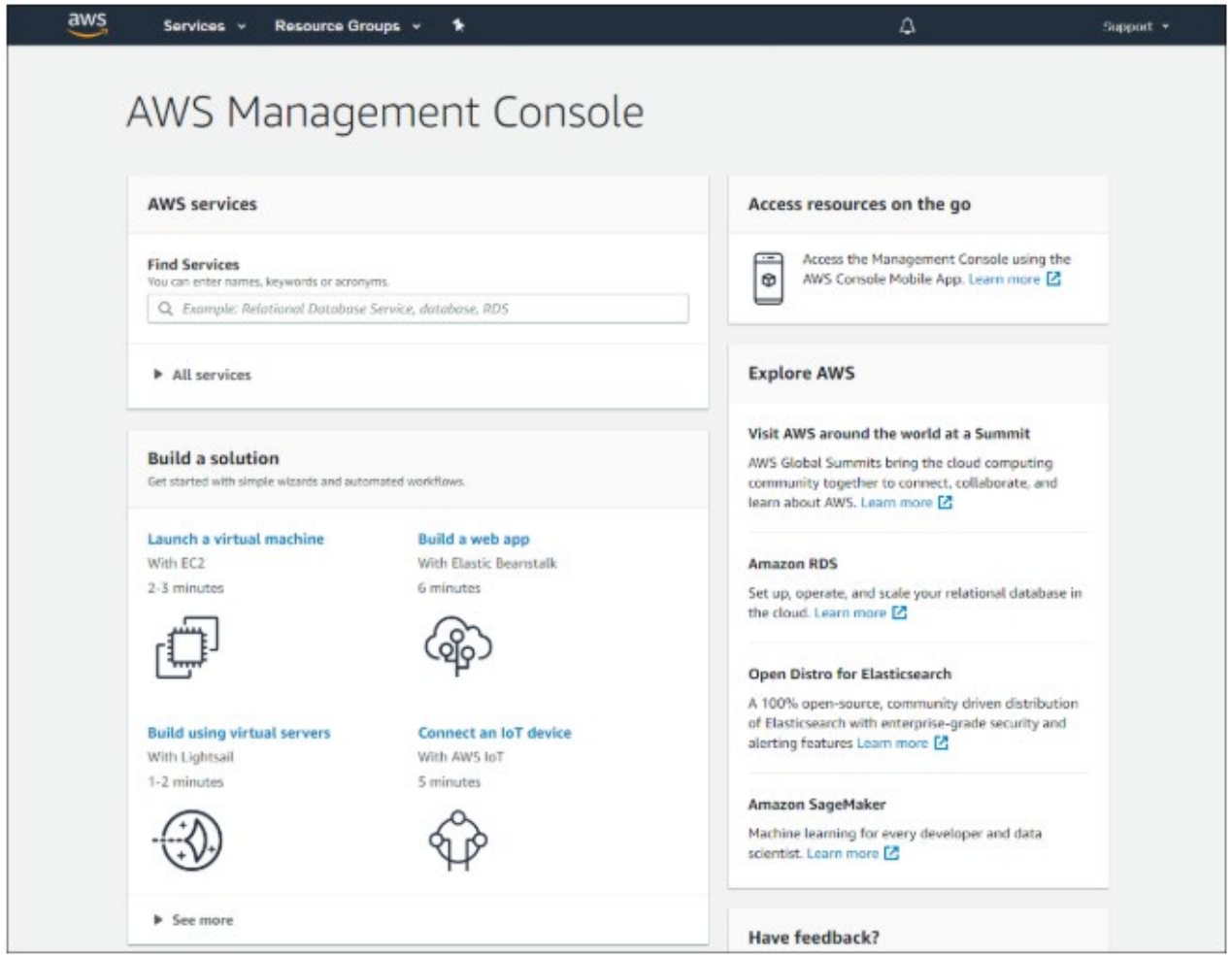
Облачные вычисления. Как правило, размещенный не на территории заказчика сервис, который предоставляет доступ по запросу к совместно используемому пулу настраиваемых вычислительных ресурсов. Эти ресурсы можно быстро выделять и освобождать с минимальными усилиями по управлению.

Центры обработки данных — это физические средства, которые обеспечивают вычислительные, сетевые и складские потребности облачных вычислений. Поставщики облачных сервисов используют центры обработки данных для размещения своих облачных сервисов и облачных ресурсов.

13.2 ВИРТУАЛИЗАЦИЯ
13.2.1 ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ И ВИРТУАЛИЗАЦИЯ

Термины «облачные вычисления» и «виртуализация» нередко используются взаимозаменяемо, однако значение у них разное. **Виртуализация** — это основа облачных вычислений. Без нее облачные вычисления в наиболее распространенных сегодня вариантах реализации были бы попросту невозможны.

Виртуализация отделяет операционную систему от аппаратного обеспечения. Различные поставщики предоставляют облачные виртуальные сервисы, в которых серверы могут предоставляться динамически, в соответствии с потребностью в них. Соответствующие виртуализированные экземпляры серверов создаются по запросу.



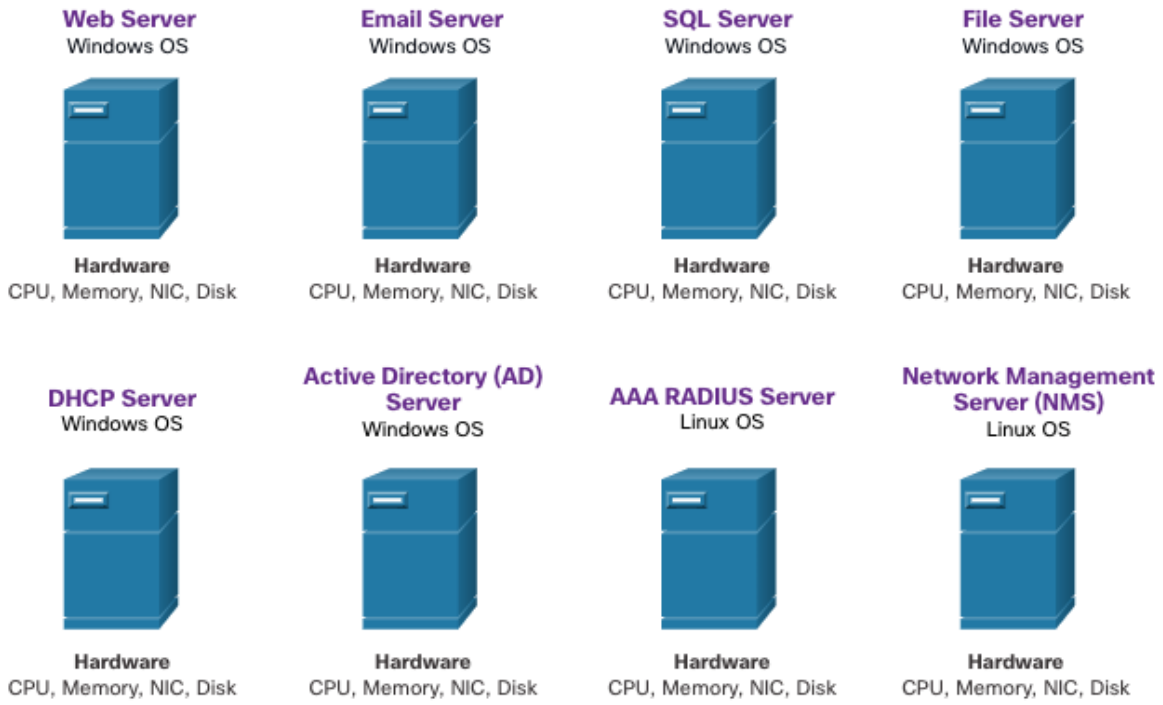
13.2.2 ВЫДЕЛЕННЫЕ СЕРВЕРЫ

Исторически сложилось так, что корпоративные серверы состояли из серверной операционной системы, например Windows Server или серверного варианта Linux, установленных на специфическое аппаратное обеспечение. Оперативная память, процессорная мощность и дисковое пространство выделялись для предоставляемых сервисов (например, Интернет, электронная почта и пр.).

Когда на каком-либо компоненте возникает сбой, сервис, предоставляемый этим сервером, становится недоступным. Такая конфигурация называется конфигурацией с единой точкой отказа.

13.2.2 ВЫДЕЛЕННЫЕ СЕРВЕРЫ

Выделенные серверы, как правило, используются недостаточно. Они часто находились в течение долгого времени в состоянии простоя, ожидая запроса на предоставление соответствующего сервиса. Эти серверы тратили впустую энергию и занимали больше места, чем было обусловлено количеством предоставляемых услуг. Такая ситуация называется разрастанием числа серверов.

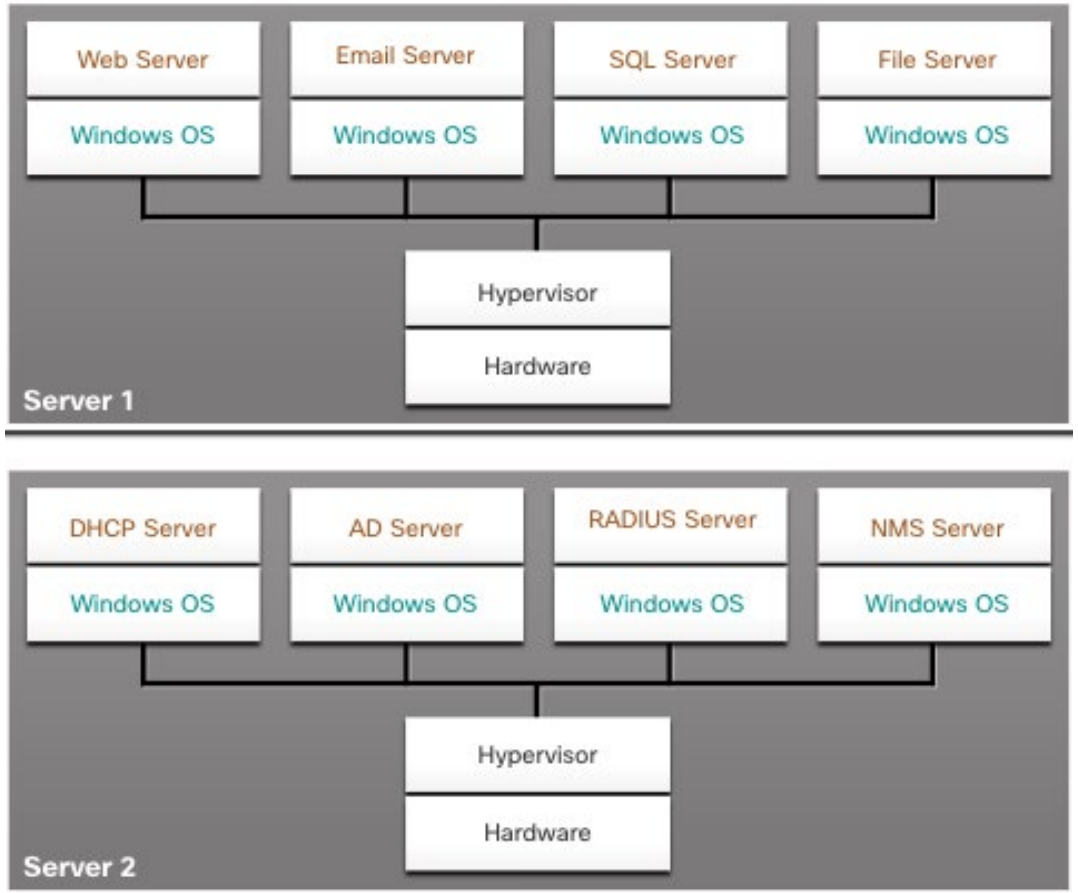


13.2.3 ВИРТУАЛИЗАЦИЯ СЕРВЕРОВ

Виртуализация серверов позволяет использовать незадействованные ресурсы и объединяет несколько необходимых серверов. Она позволяет размещать и запускать несколько операционных систем на одной аппаратной платформе.

Использование виртуализации обычно предусматривает резервирование, чтобы избежать ситуации с единой точкой отказа.

Гипервизор — это программа, встроенное ПО или аппаратные средства, которые добавляют уровень абстракции поверх реальных физических аппаратных средств. Этот уровень абстракции используется для создания виртуальных машин, которые имеют доступ ко всем аппаратным средствам физического компьютера, включая ЦП, память, контроллеры дисков и сетевые интерфейсные платы.



13.2.4 ПРЕИМУЩЕСТВА ВИРТУАЛИЗАЦИИ

Одним из главных преимуществ виртуализации является общее снижение расходов.

Требуется меньше оборудования.

Потребляется меньше энергии.

Требуется меньше места.

Ниже перечислены дополнительные преимущества виртуализации.

Упрощенное моделирование.

Более быстрое выделение ресурсов сервера.

Сокращение простоев сервера.

Улучшение возможностей аварийного восстановления.

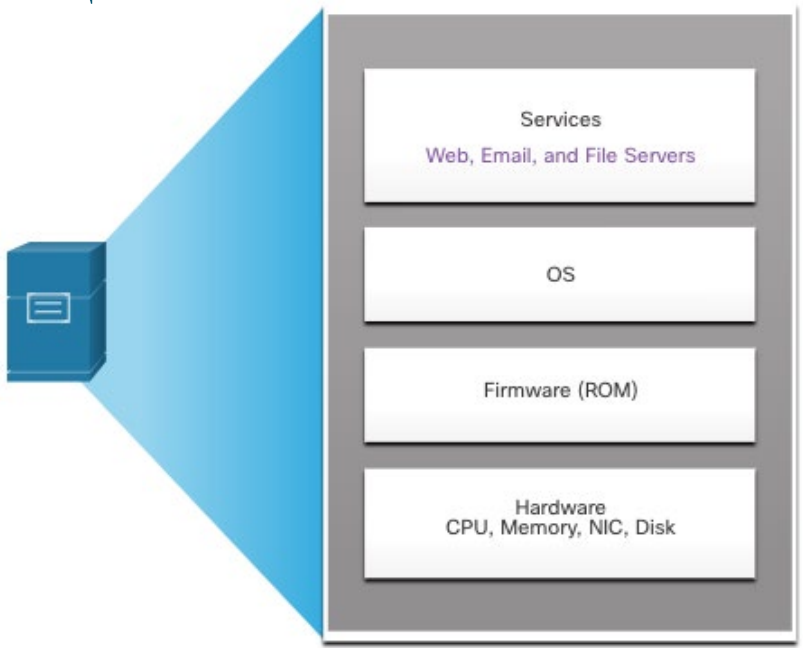
Поддержка снятого с производства оборудования.

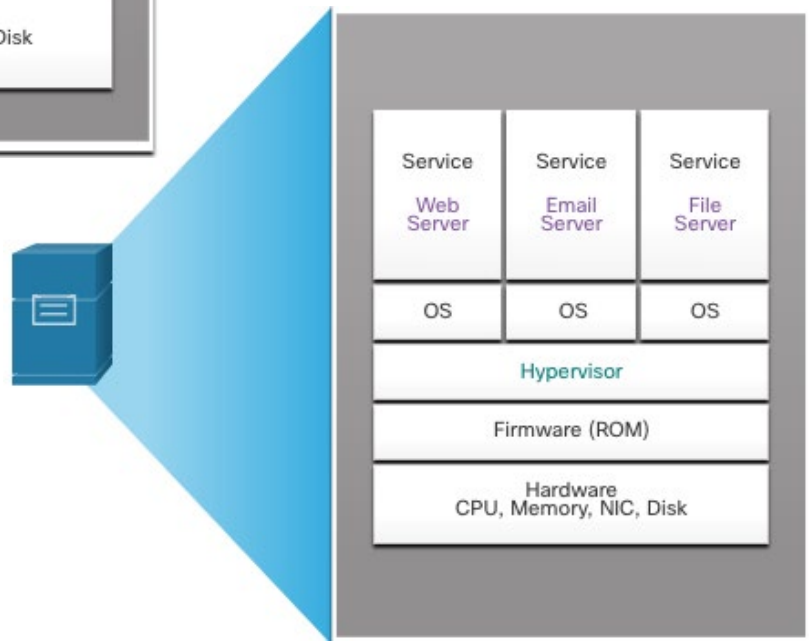
13.2.5 УРОВНИ АБСТРАКЦИИ

Компьютерная система состоит из следующих уровней абстракции: сервисов, ОС, микропрограмм и оборудования.

На каждом из этих уровней абстракции используется определенный тип программного кода в качестве интерфейса между уровнем ниже и уровнем выше.

Между микропрограммой и операционной системой установлен гипервизор. Гипервизор поддерживает несколько экземпляров ОС.

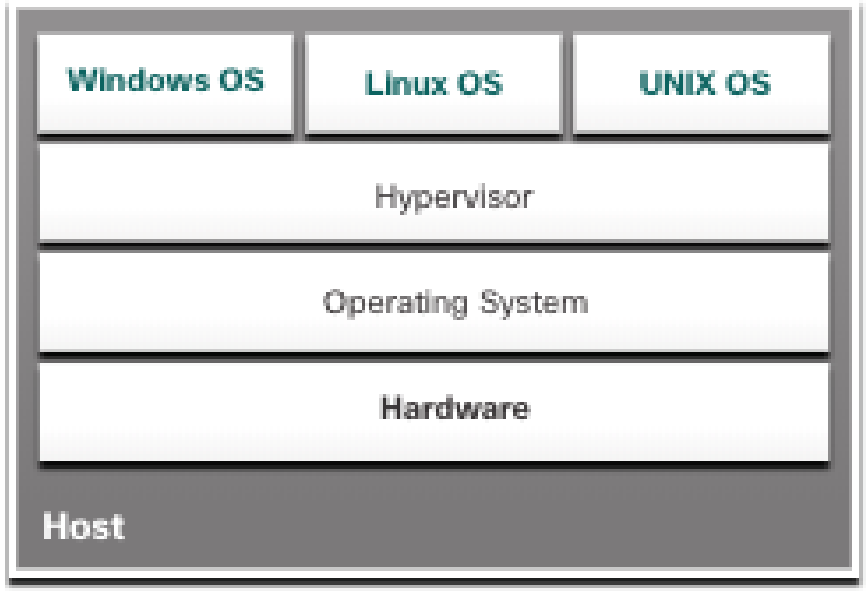




13.2.6 ГИПЕРВИЗОРЫ ТИПА 2

Гипервизор типа 2 — это программное обеспечение, которое создает и обеспечивает работу экземпляров виртуальных машин. Компьютер, в котором гипервизор поддерживает одну или несколько виртуальных машин, называется хостом (хост-компьютером). Гипервизоры типа 2 также называются гипервизорами на основе базовой ОС.

Главное преимущество гипервизоров типа 2 состоит в том, что при их использовании не требуется консоль управления.

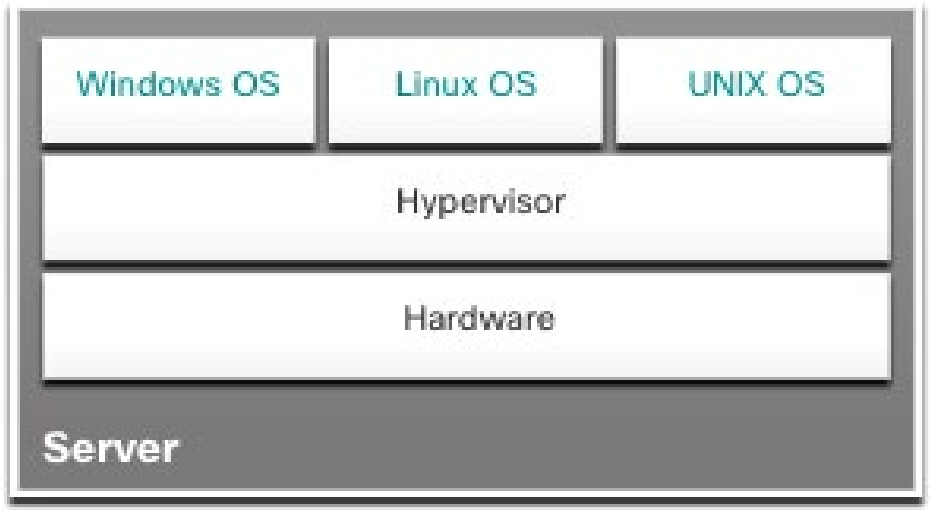


13.3 ВИРТУАЛЬНАЯ СЕТЕВАЯ ИНФРАСТРУКТУРА

13.3.1 ГИПЕРВИЗОРЫ ТИПА 1

В **гипервизорах типа 1** используется подход bare metal (без ОС). Он называется так потому, что гипервизор устанавливается непосредственно на аппаратную часть. Гипервизоры типа 1 обычно используются на серверах предприятия и сетевых устройствах центра обработки данных.

Гипервизоры типа 1 устанавливаются непосредственно на физическом сервере или сетевом оборудовании. После этого экземпляры ОС устанавливаются на гипервизор, как показано на рисунке. Гипервизоры типа 1 имеют прямой доступ к аппаратным ресурсам. Поэтому они более эффективны, чем размещенные архитектуры. Гипервизоры типа 1 отличаются повышенной масштабируемостью, производительностью и надежностью.



13.3.2 УСТАНОВКА ВИРТУАЛЬНОЙ МАШИНЫ НА ГИПЕРВИЗОРЕ

Для управления гипервизорами типа 1 требуется «консоль управления». Управляющее программное обеспечение позволяет управлять несколькими серверами, использующими один и тот же гипервизор. Консоль управления может автоматически объединять, включать и выключать серверы по мере необходимости.

Консоль управления обеспечивает восстановление после аппаратного сбоя. При выходе из строя серверного компонента консоль управления автоматически переносит виртуальную машину на другой сервер. Система управления Cisco UCS Manager управляет множеством серверов, а также выделяет ресурсы для тысяч виртуальных машин.

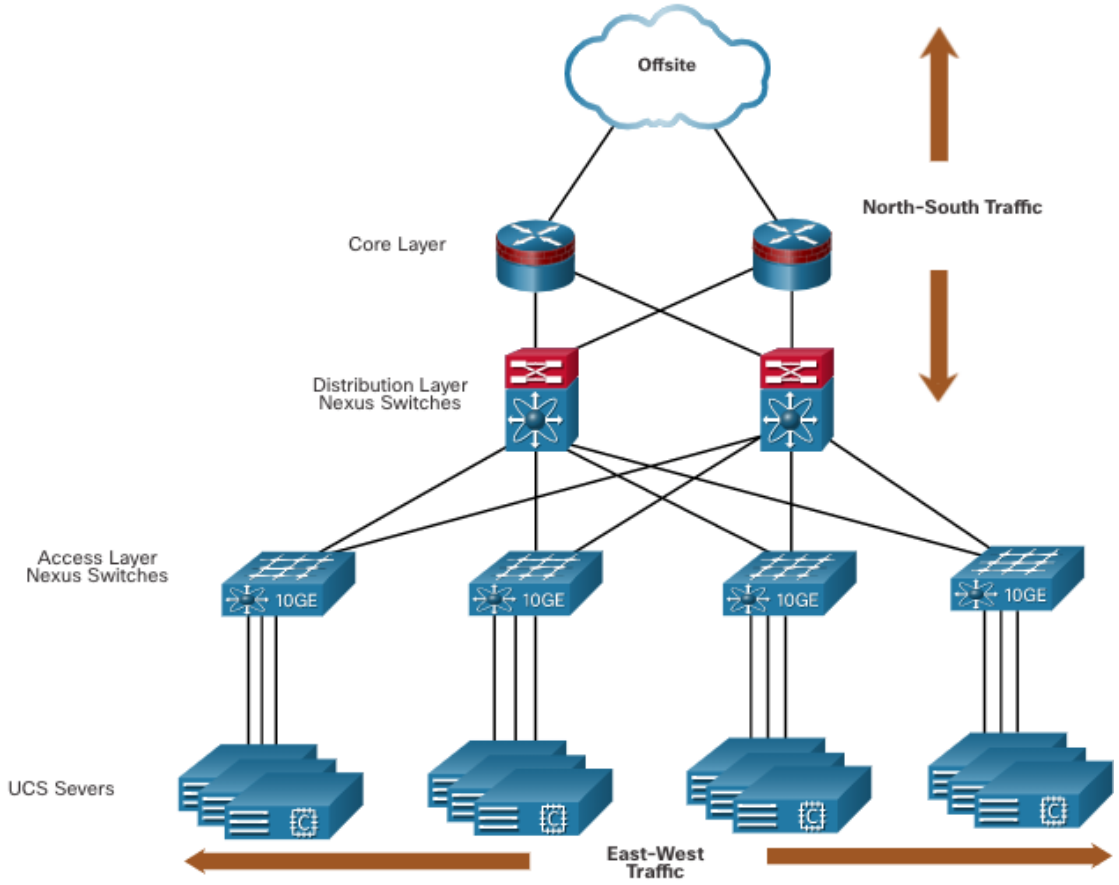
Некоторые консоли управления также позволяют серверу настраивать переподписку ресурсов. Переподписка ресурсов возникает, когда установлено несколько экземпляров операционной системы и выделенный им объем памяти превышает общий объем физической памяти на сервере. Перераспределение является обычной практикой, потому что все четыре экземпляра ОС редко требуют все свои выделенные ресурсы в любой момент.

13.3.3 КОМПЛЕКСНАЯ ВИРТУАЛИЗАЦИЯ СЕТИ

Виртуализация серверов скрывает серверные ресурсы. Когда используются традиционные сетевые архитектуры, могут возникать проблемы.

Однако виртуальные машины могут переноситься, и сетевой администратор должен иметь возможность добавлять, удалять и изменять сетевые ресурсы и профили. Этот процесс будет ручным и трудоемким с традиционными сетевыми коммутаторами.

Потоки трафика отличаются от традиционной модели клиент-сервер. Как правило, происходит обмен значительным объемом трафика между виртуальными серверами (трафик Восток-Запад), который со временем меняется в местоположении и интенсивности. Трафик Север-Юг обычно предназначен для удаленных местоположений, таких как другой центр обработки данных, другие поставщики облачных услуг или Интернет.



13.3.3 КОМПЛЕКСНАЯ ВИРТУАЛИЗАЦИЯ СЕТИ

Динамический постоянно меняющийся трафик требует гибкого подхода к управлению сетевыми ресурсами. Существующие сетевые инфраструктуры могут реагировать на меняющиеся требования, связанные с управлением потоками трафика, с помощью механизмов качества обслуживания (QoS) и конфигураций уровня безопасности для отдельных потоков. Однако на крупных предприятиях, использующих оборудование от различных поставщиков, при добавлении каждой новой виртуальной машины необходимые изменения конфигурации могут занимать очень много времени.

Сетевая инфраструктура может также пользоваться преимуществами виртуализации? Сетевые функции могут быть виртуализированы. Каждое сетевое устройство может быть разделено на несколько виртуальных устройств, которые работают как независимые устройства. Примеры включают субинтерфейсы, виртуальные интерфейсы, VLAN и таблицы маршрутизации. Виртуализированная маршрутизация называется виртуальная маршрутизация и переадресация (VRF - virtual routing and forwarding).

13.4 ПРОГРАММНО-ОПРЕДЕЛЯЕМЫЕ СЕТИ

13.4.1 УРОВЕНЬ УПРАВЛЕНИЯ И УРОВЕНЬ ПЕРЕДАЧИ ДАННЫХ

Сетевое устройство содержит следующие уровни:

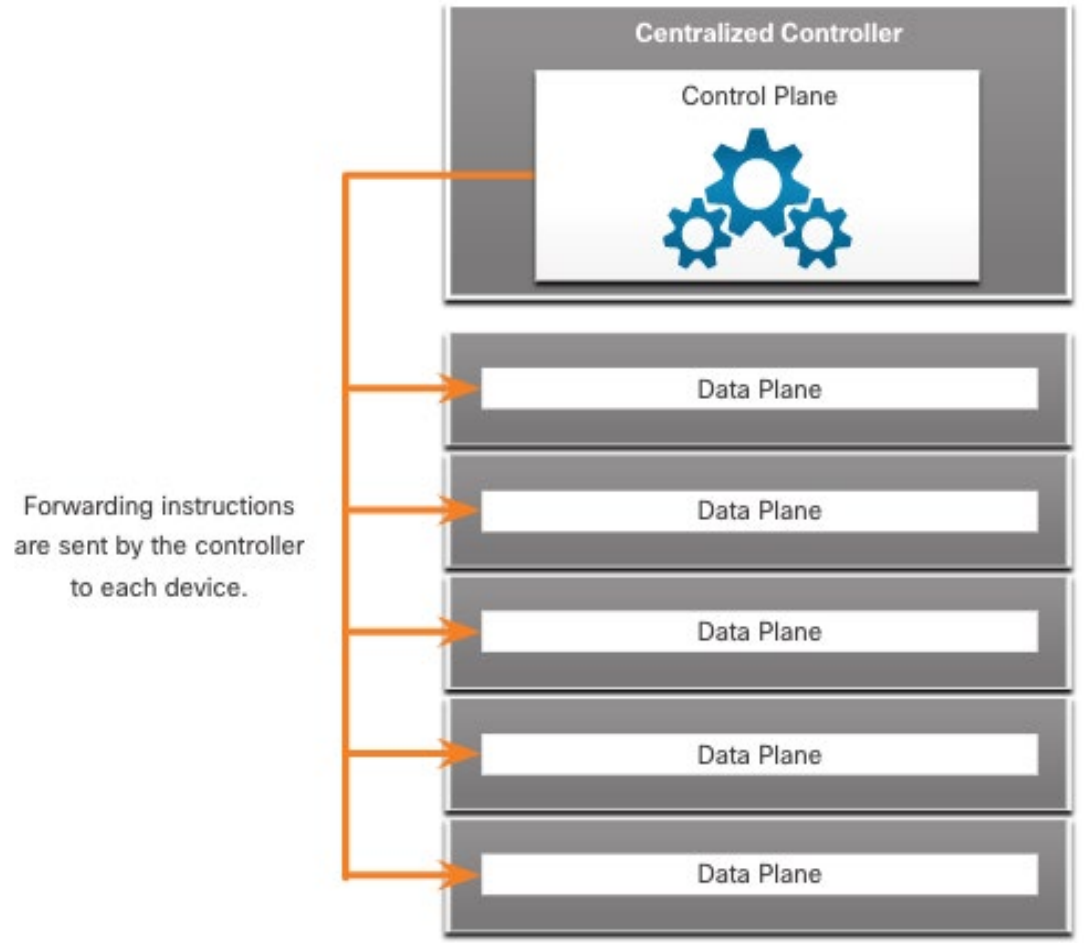
Уровень управления — обычно считается мозгом устройства. Он принимает решения о пересылке данных. Уровень управления содержит механизмы пересылки уровня 2 и уровня 3, например таблицы соседей протокола маршрутизации и таблицы топологии, таблицы маршрутизации IPv4 и IPv6, STP и таблицу ARP. Данные, передаваемые на уровень управления, обрабатываются ЦП.

Уровень передачи данных — этот уровень, также называемый уровнем пересылки, обычно представляет коммутационную структуру, которая связывает разные сетевые порты на устройстве. Уровень передачи данных каждого устройства используется для пересылки потоков трафика. Маршрутизаторы и коммутаторы используют данные уровня управления для пересылки входящего трафика на соответствующий выходной интерфейс. Информация в плоскости данных обычно обрабатывается специальным процессором плоскости данных без участия ЦП.

13.4.1 УРОВЕНЬ УПРАВЛЕНИЯ И УРОВЕНЬ ПЕРЕДАЧИ ДАННЫХ

Пересылку пакетов на уровне передачи данных без обращения к уровню управления обеспечивает CEF — технология IP-коммутации уровня 3.

SDN — это в основном разделение плоскости управления и плоскости данных. Для виртуализации сети с каждого устройства удаляется функция уровня управления, которую начинает исполнять один централизованный контроллер. Централизованный контроллер передает команды уровня управления каждому устройству. Теперь каждое устройство может сосредоточиться на пересылке данных, а централизованный контроллер управляет потоком данных, повышает безопасность и предоставляет другие услуги.



13.4.1 УРОВЕНЬ УПРАВЛЕНИЯ И УРОВЕНЬ ПЕРЕДАЧИ ДАННЫХ

Уровень управления отвечает за управление устройством через его подключение к сети.

Сетевые администраторы используют такие приложения, как Secure Shell (SSH), Trivial File Transfer Protocol (TFTP), Secure FTP и Secure Hypertext Transfer Protocol (HTTPS) для доступа к уровню управления и настройки устройства.

Уровень управления - это то, как вы обращались к устройствам и настраивали их в своих сетевых исследованиях. Кроме того, такие протоколы, как протокол SNMP, используют уровень управления.

13.4.2 ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ СЕТЕЙ

Для поддержки виртуализации сети разработаны две основные сетевые архитектуры:

Программно-определяемая сеть (SDN) — сетевая архитектура, которая виртуализирует сеть, предлагая новый подход к сетевому администрированию и управлению, направленный на упрощение и оптимизацию процесса администрирования.

Ориентированная на приложения архитектура Cisco (ACI) — специализированное аппаратное решение для интеграции облачных вычислений и управления ЦОД.

13.4.2 ТЕХНОЛОГИИ ВИРТУАЛИЗАЦИИ СЕТЕЙ

Компоненты SDN могут включать следующее:

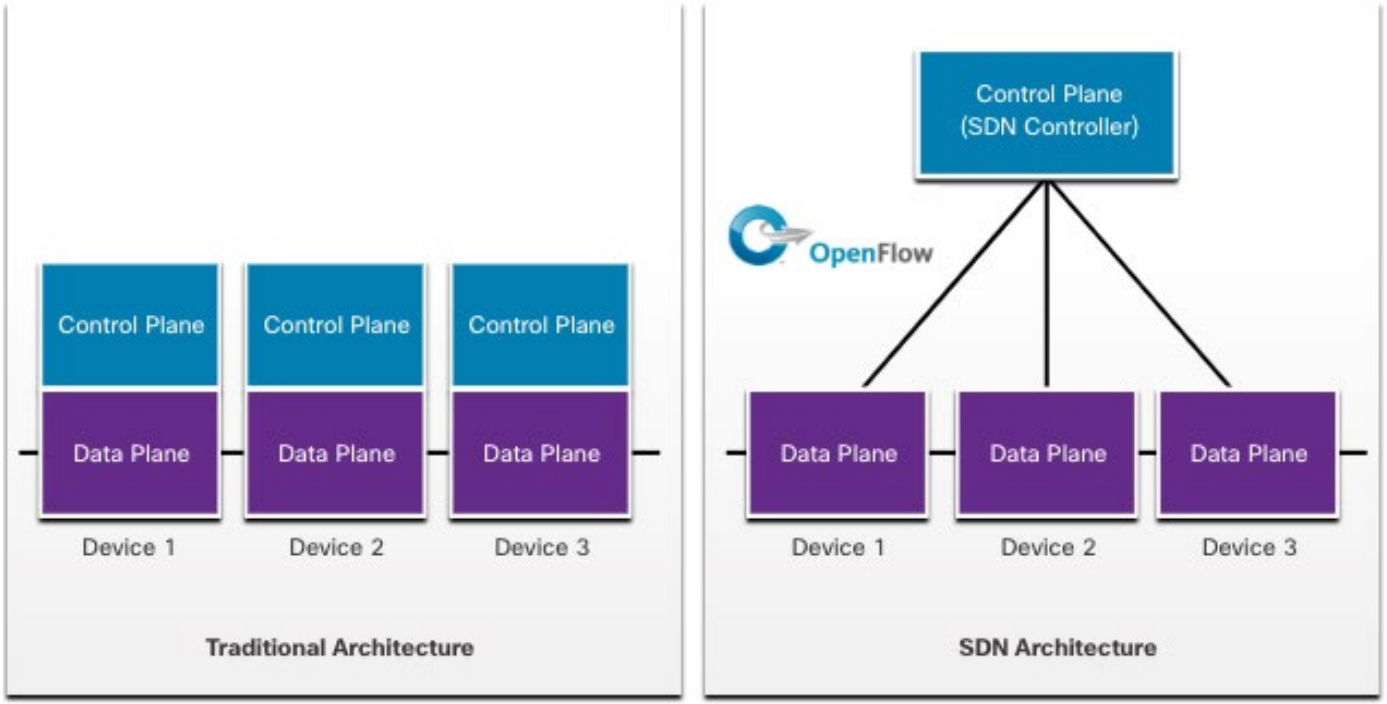
OpenFlow. Этот подход был разработан в Стэнфордском университете для управления трафиком между маршрутизаторами, коммутаторами, точками беспроводного доступа и контроллером. **Протокол OpenFlow** — это базовый элемент в построении решений SDN.

OpenStack. Этот подход представляет собой платформу виртуализации и оркестровки, предназначенную для создания масштабируемых облачных сред и предоставления решения IaaS. OpenStack часто используется с Cisco ACI. **Оркестрации в сети** — это процесс автоматизации выделения сетевых компонентов, таких как серверы, хранилища, коммутаторы, маршрутизаторы и приложения.

Другие компоненты — включают интерфейс с системой маршрутизации (I2RS), прозрачную взаимосвязь с большим числом каналов (TRILL), Cisco FabricPath (FP), а также построение мостов по кратчайшему пути IEEE 802.1aq (SPB).

13.4.3 ТРАДИЦИОННАЯ АРХИТЕКТУРА И АРХИТЕКТУРА SDN

В традиционной маршрутизируемой или коммутируемой архитектуре функции уровня управления и уровня передачи данных объединены на одном устройстве. Решения о маршрутизации и пересылке пакетов принимаются операционной системой устройства. В SDN управление уровнем управления перемещается на централизованный контроллер SDN. На рисунке сравнивается традиционная и SDN архитектуры.



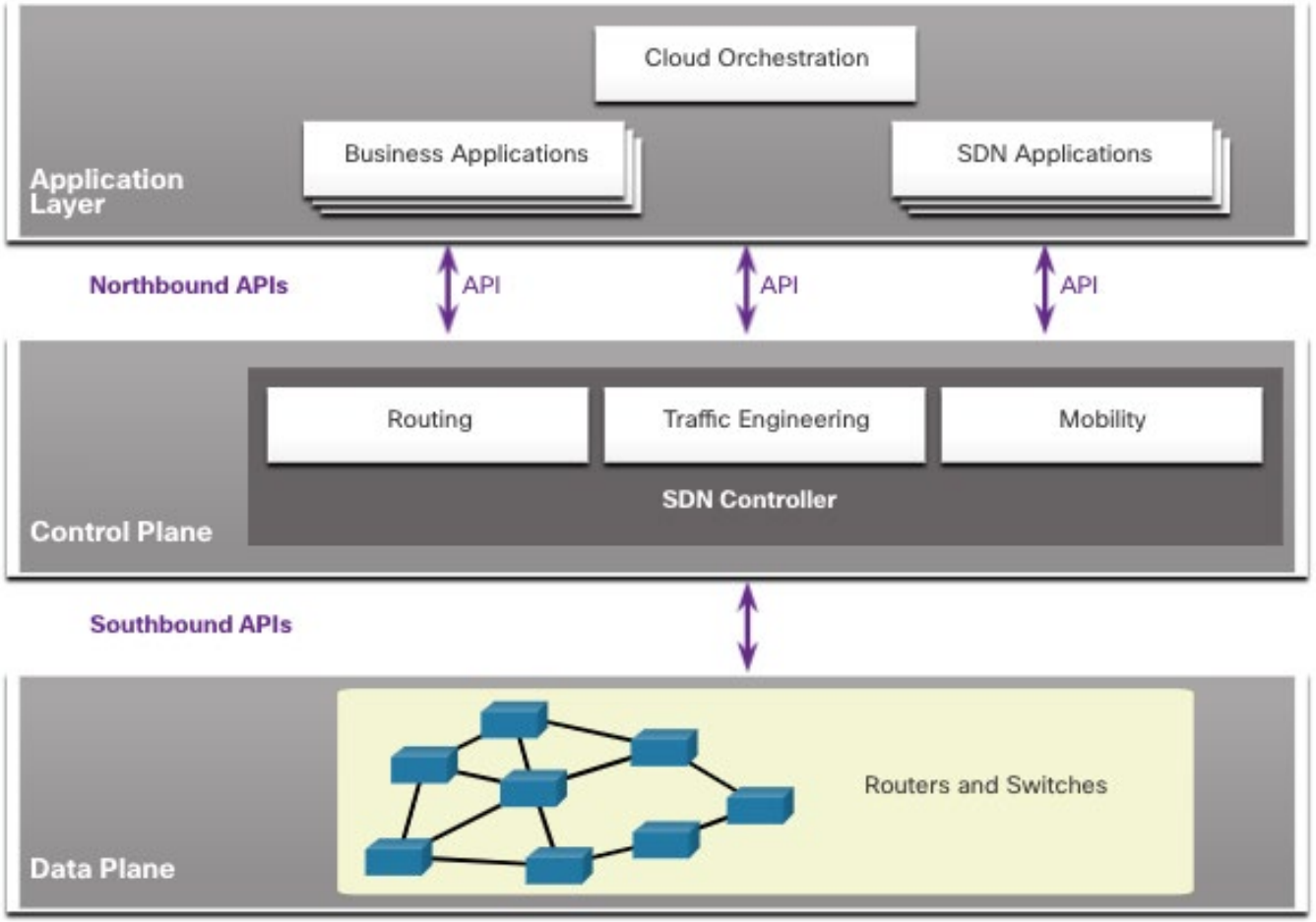
13.4.3 ТРАДИЦИОННАЯ АРХИТЕКТУРА И АРХИТЕКТУРА SDN

Контроллер SDN — это логическая сущность, которая позволяет сетевым администраторам определять, как уровень передачи данных на коммутаторах и маршрутизаторах будет обрабатывать сетевой трафик. Он координирует, служит посредником и организует взаимодействие между приложениями и сетевыми элементами.

Полная структура SDN показана на рисунке. Обратите внимание на использование программных интерфейсов (API). API — это набор стандартизованных запросов, которые задают для

13.4.3 ТРАДИЦИОННАЯ АРХИТЕКТУРА И АРХИТЕКТУРА SDN

Контроллер SDN использует «северные» API-интерфейсы для обмена данными с вышестоящими приложениями, помогая сетевым администраторам формировать трафик и развертывать сервисы. Контроллер SDN также использует «южные» API-интерфейсы для определения поведения уровней данных на нисходящих коммутаторах и маршрутизаторах. OpenFlow — это широко используемый «южный» API-интерфейс.

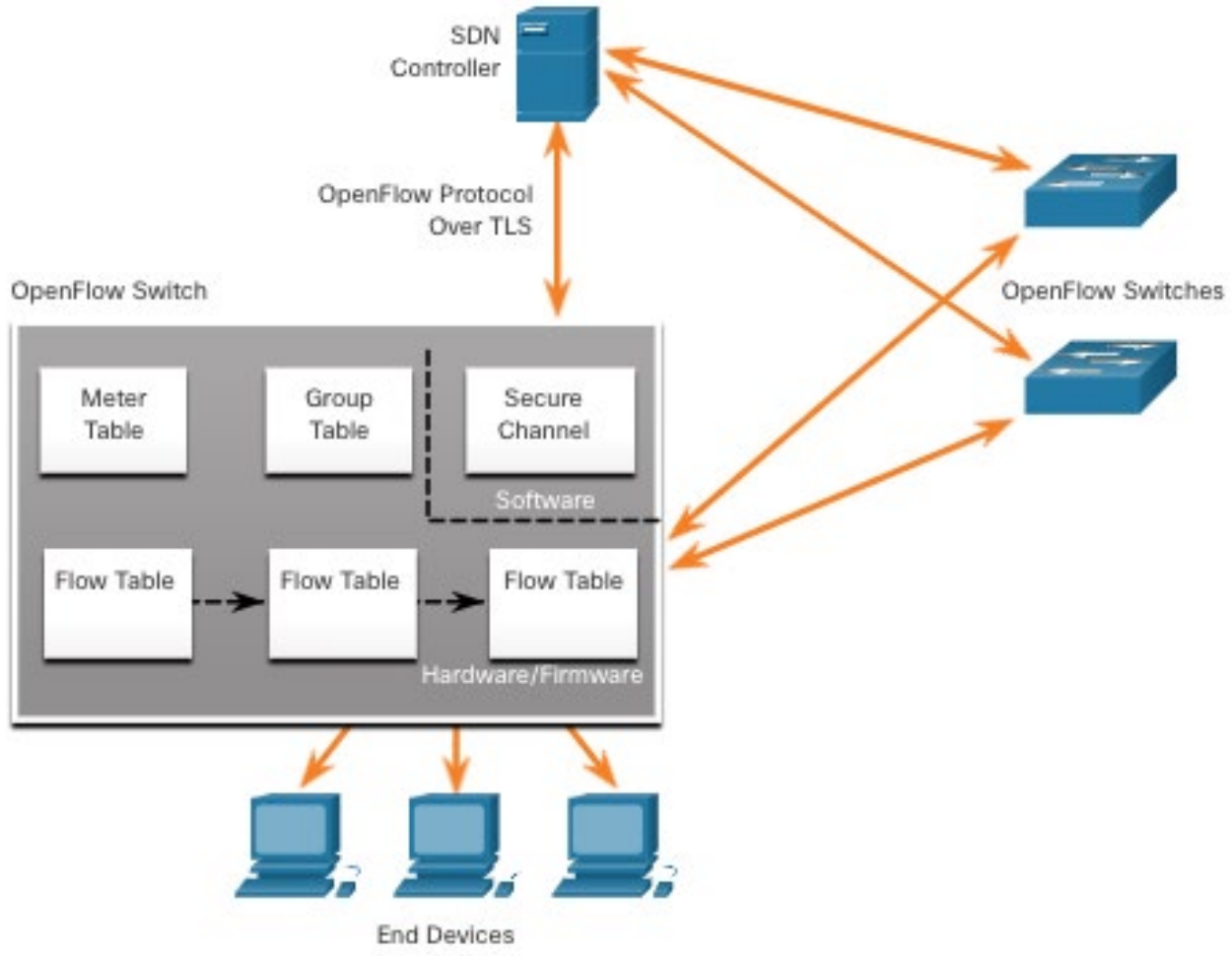


13.5 КОНТРОЛЛЕРЫ
13.5.1 КОНТРОЛЛЕР И ОПЕРАЦИИ SDN

Контроллер SDN определяет потоки данных между централизованным уровнем управления и уровнями передачи данных на отдельных маршрутизаторах и коммутаторах.

Каждый из потоков, проходящих по сети, сначала должен получить разрешение от контроллера SDN, который проверяет, разрешен ли такой обмен данными в соответствии с сетевыми политиками.

Все сложные функции выполняются контроллером. Контроллер заполняет таблицы потоков. Коммутаторы управляют таблицами потоков.



13.5.1 КОНТРОЛЛЕР И ОПЕРАЦИИ SDN

В каждом коммутаторе имеется набор таблиц, реализованных на уровне аппаратных средств, или микропрограммы, которые используются для управления потоками пакетов через коммутатор. Для коммутатора поток представляет собой последовательность пакетов, которая соответствует определенной записи в таблице потоков.

Три типа таблиц, показанные на предыдущем рисунке, являются следующими:

Таблица потоков. Используется для сопоставления входящих пакетов с конкретным потоком и определения функций, которые выполняются для пакетов. Возможно наличие нескольких таблиц потоков, которые работают как конвейер.

Таблица групп. Таблица потоков может направлять поток в таблицу групп, которая может запускать различные действия, влияющие на один или несколько потоков.

Таблица счетчиков. Запускает различные, связанные с производительностью операции в потоке, включая возможность ограничения скорости трафика.

13.5.2 CISCO ACI

На деле лишь немногие организации хотят программировать сети с помощью средств SDN или обладают для этого достаточной квалификацией. Однако большинство организаций хотят автоматизировать сеть, ускорить развертывание приложений и привести свою ИТ-инфраструктуру в соответствие с бизнес-требованиями. Компания Cisco разработала ориентированную на приложения инфраструктуру (ACI), чтобы решать эти задачи более современными и инновационными способами, чем те, которые основаны на SDN.

Архитектура Cisco ACI — это специализированное аппаратное решение для интеграции облачных вычислений и управления ЦОД. На верхнем уровне элемент управления политиками сети удаляется из уровня передачи данных. Это упрощает создание сетей центра обработки данных.

13.5.3 ОСНОВНЫЕ КОМПОНЕНТЫ ИНФРАСТРУКТУРЫ ACI

Три основных компонента архитектуры ACI:

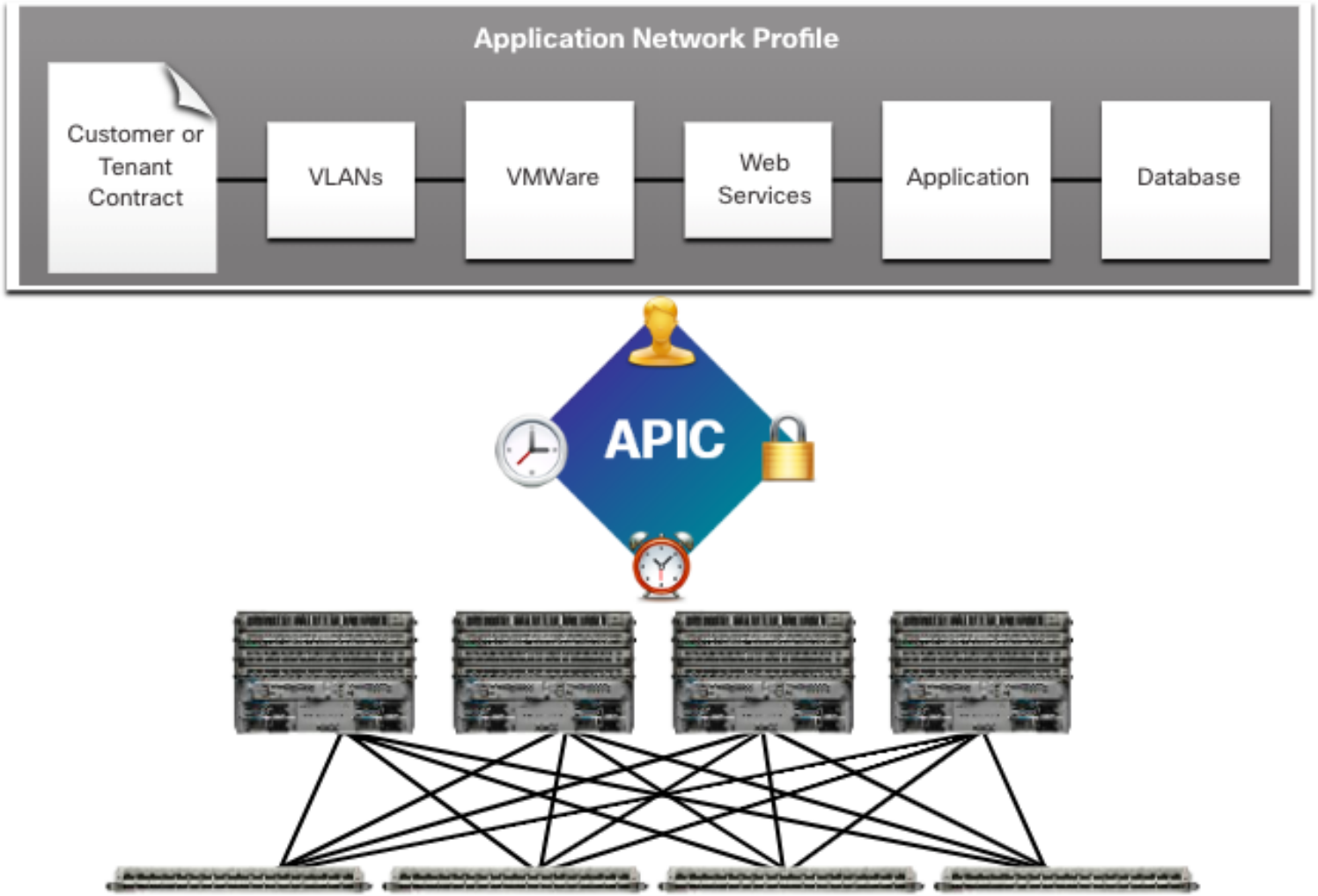
Сетевой профиль приложения (ANP) — это набор групп оконечных устройств (EPG), их подключений, а также политик, определяющих эти подключения.

Контроллер Cisco APIC — это централизованный программный контроллер, который управляет масштабируемой кластеризованной структурой ACI. Он разработан для обеспечения возможности программирования и централизованного управления. Он преобразует политики приложений в сетевой программный код.

Коммутаторы Cisco Nexus серии 9000 — эти коммутаторы реализуют коммутационную структуру с учетом работы приложений и работают совместно с контроллером Cisco APIC, обеспечивая управление инфраструктурой виртуальной и физической сети.

Контроллер APIC располагается между ANP и сетевой инфраструктурой ACI. APIC преобразует требования приложений в настройке сети, соответствующей этим требованиям.

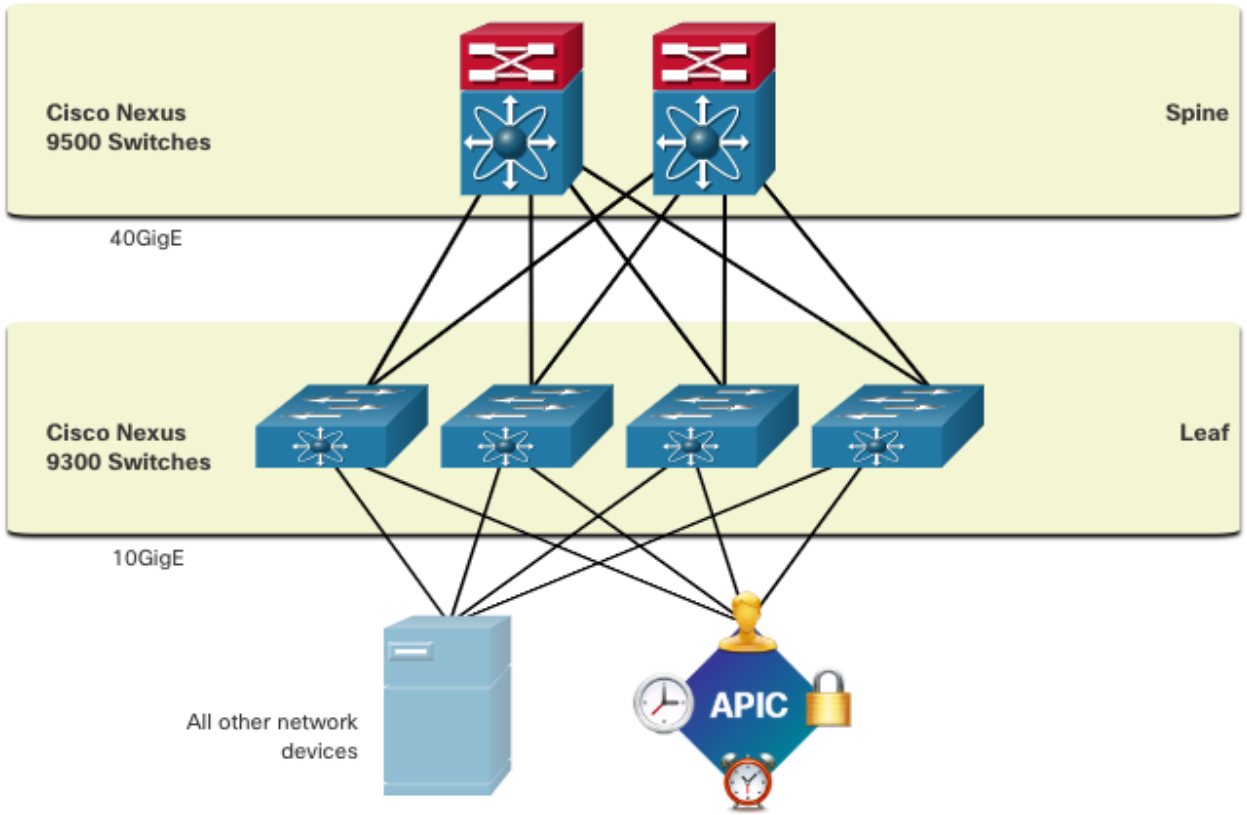
13.5.3 ОСНОВНЫЕ КОМПОНЕНТЫ ИНФРАСТРУКТУРЫ ACI



13.5.4 ТОПОЛОГИЯ «СТВОЛ-ЛИСТЬЯ» (SPINE-LEAF)

Структура Cisco ACI состоит из контроллера APIC и коммутаторов Cisco Nexus серии 9000, использующих двухуровневую топологию «ствол и листья», как показано на рисунке. Коммутаторы-«листья» всегда соединяются со стволовыми коммутаторами, но никогда не соединяются друг с другом. Аналогично стволовые коммутаторы соединяются только с листовыми и базовыми коммутаторами (не показано). В этой двухъярусной топологии любой узел находится в одном переходе от любого другого узла.

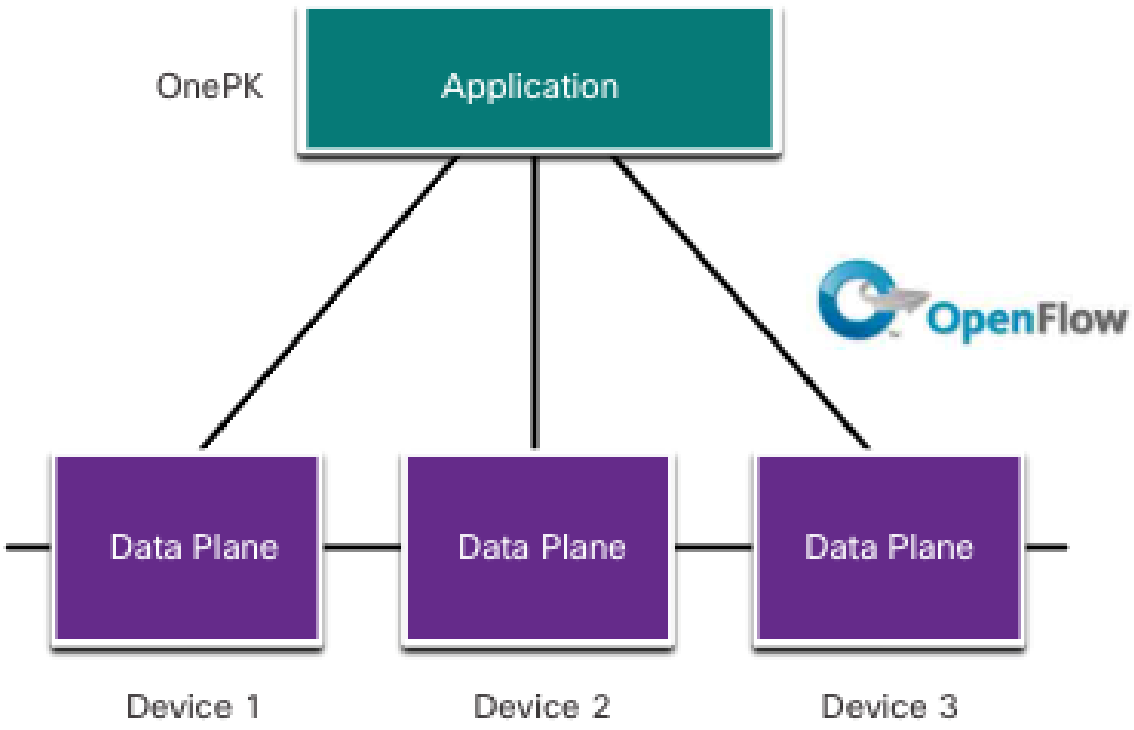
В отличие от SDN, контроллер APIC напрямую не управляет каналом данных. Вместо этого APIC обеспечивает централизованное хранение определений политик и программирует листовые коммутаторы на пересылку трафика с учетом определенных политик.



13.5.5 ТИПЫ SDN

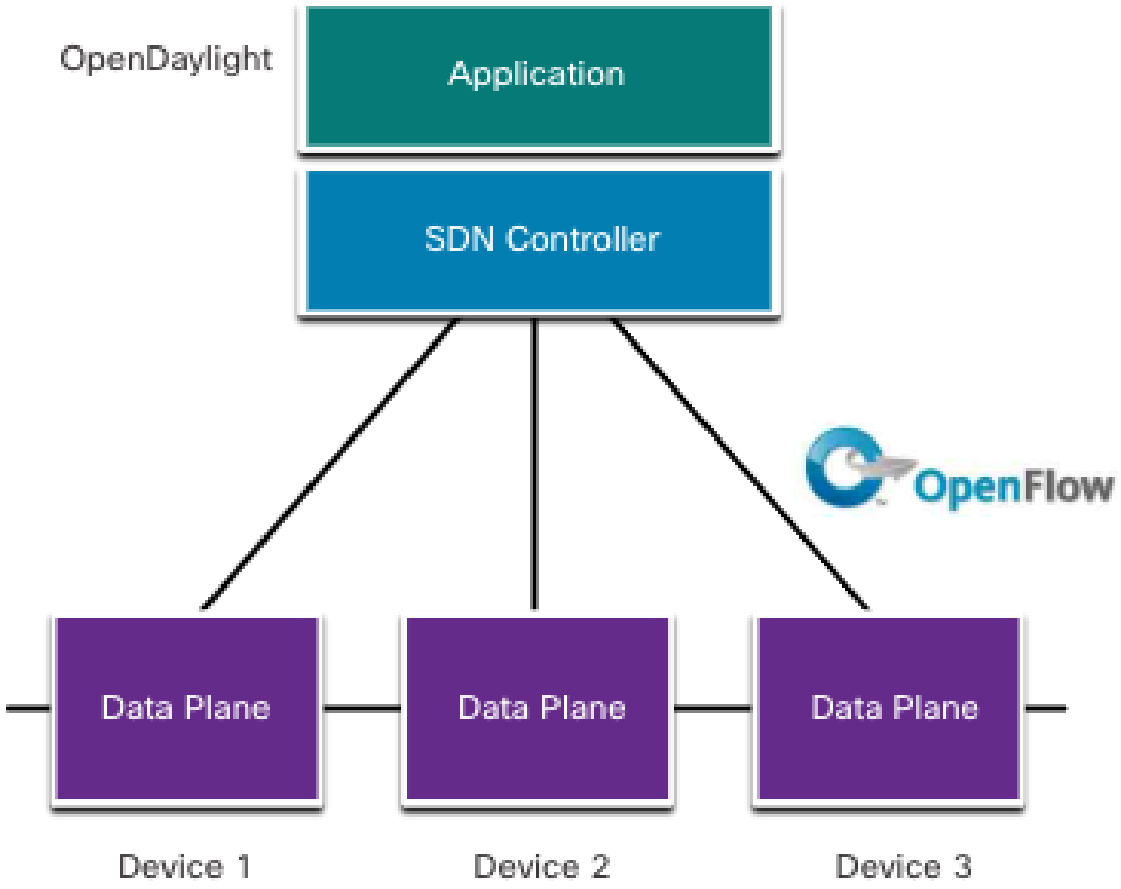
Модуль контроллера Cisco Application Policy Infrastructure Controller — Enterprise Module (**APIC-EM**) расширяет ACI функционалом, рассчитанным на развертывание в корпоративных средах и средах комплексов зданий. Для лучшего понимания APIC-EM будет полезно взглянуть со стороны на три типа сетей SDN.

1. SDN на основе устройств. Устройства программируются приложениями, работающими на самом устройстве или на сервере в сети, как показано на рисунке.



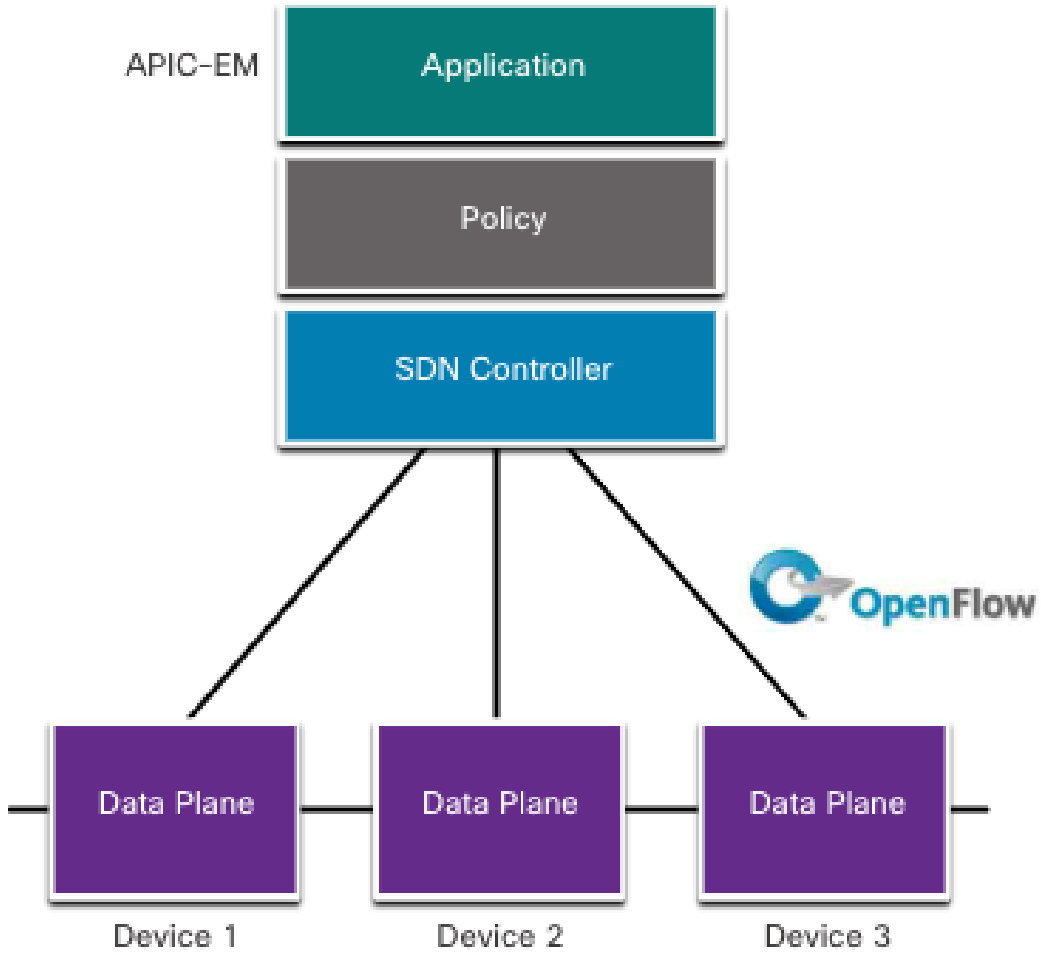
13.5.5 ТИПЫ SDN

2. SDN на основе контроллера — в этом типе сетей SDN используется централизованный контроллер, которому известны все устройства в сети, как показано на рисунке. Приложения могут взаимодействовать с контроллером, отвечающим за управление устройствами и обработку потоков трафика в сети. Контроллер Cisco Open SDN является коммерческим дистрибутивом OpenDaylight.



13.5.5 ТИПЫ SDN

3. SDN на основе политик. Аналогичны сетям SDN на основе контроллера, в котором централизованному контроллеру доступно представление всех устройств в сети, как показано на рисунке. SDN на базе политик включает дополнительный уровень политик, который работает на более высоком уровне абстракции. Он использует встроенные приложения, которые автоматизируют задачи настройки с помощью управляемого рабочего процесса и удобного графического интерфейса пользователя. Навыки программирования не требуются. Примером такого типа SDN — Cisco APIC-EM.



13.5.6 ФУНКЦИИ APIC-EM

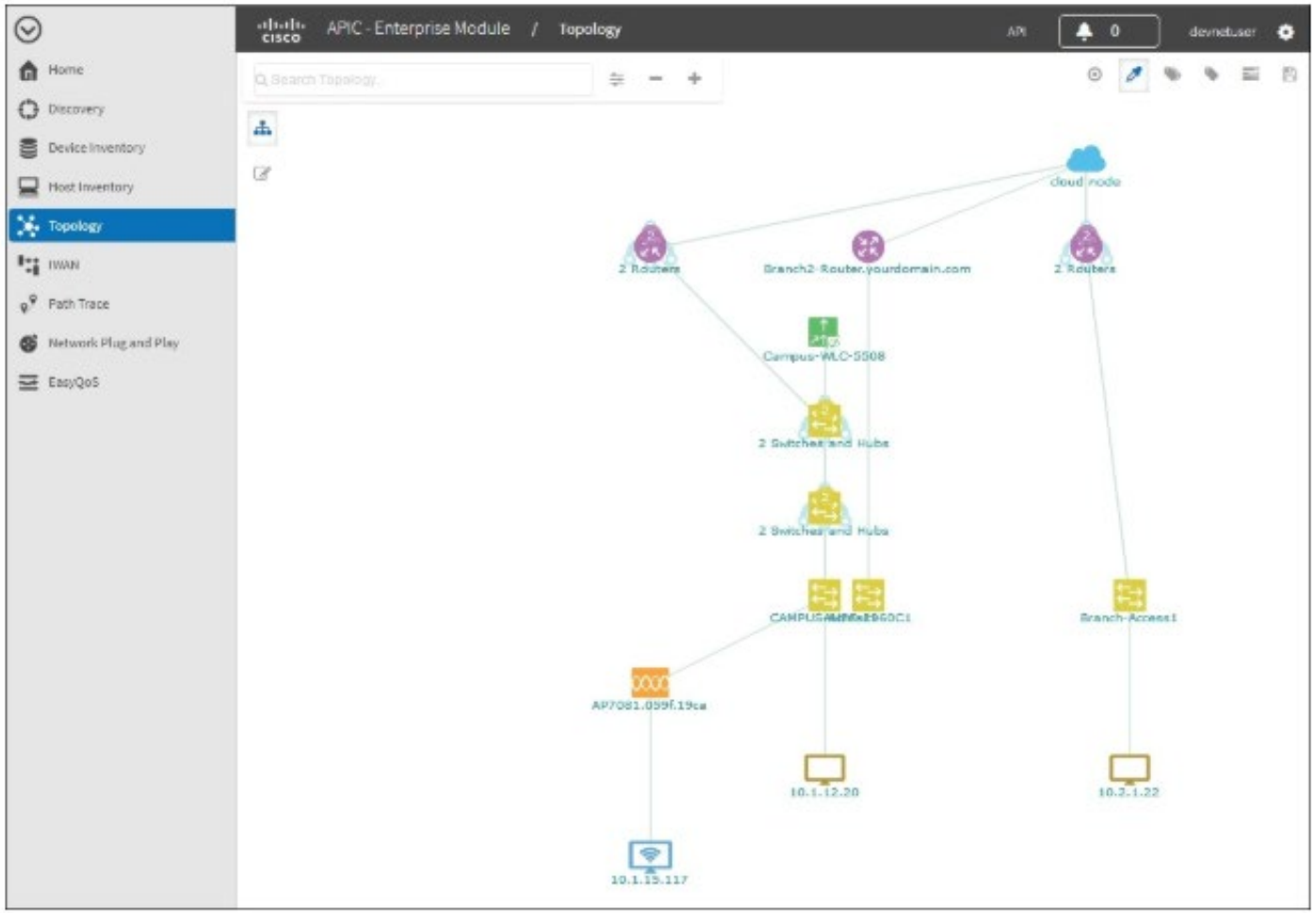
Cisco APIC-EM предоставляет единый интерфейс для управления сетью, включая:

1. Обнаружение и доступ к инвентаризации устройств и хостов.

2. Просмотр топологии (как показано на рисунке).

3. Отслеживание пути между конечными точками.

4. Политики настройки.



13.5.7 APIC-EM PATH TRACE

APIC-EM Path Trace позволяют администратору легко визуализировать потоки трафика и обнаруживать любые конфликтующие, дублированные или теневые записи ACL. Этот инструмент исследует конкретные ACL-списки на пути между двумя конечными узлами и показывает все возможные неполадки. На рисунке вы можете видеть, как любые ACL вдоль пути разрешают или запрещают трафик. Обратите внимание, как Branch-Router2 разрешает весь трафик. Теперь администратор сети может вносить коррективы, если это необходимо, для лучшей фильтрации трафика.