SDN: «ТРЕТИЙ ЭЛЕМЕНТ» ДЛЯ БУДУЩИХ ДАТА-ЦЕНТРОВ

Реализовать концепцию SDN сегодня пытаются все крупные производители сетевых решений. Но у каждого подход немного отличается, хотя и совпадает в главном. Что же такое «программно-конфигурируемая сеть» в понимании ее разработчиков и как она реализуется на практике?

Так уж сложилось исторически, что современная сетевая инфраструктура отстала от серверов и систем хранения данных в плане виртуализации, последние вовсю пользуются преимуществами данной концепции. В триаде сервер, СХД, сеть, определяющей архитектуру вычислительной системы, именно сетевой компонент оказался слабым звеном. Но ситуация начала исправляться благодаря такому явлению, как Software Define Network (SDN), в основе которого лежит открытый протокол OpenFlow. Оптимизма добавляет и тот факт, что за развитие технологии взялись все ведущие мировые разработчики сетевых решений и не только они.

О том, что такое SDN и как это работает, написано уже немало теоретических материалов (которые зачастую повторяют друг друга ввиду ничтожного числа практических реализаций в мире). Поэтому здесь мы остановимся только на ключевых особенностях технологии — тех, которые делают ее по-настоящему ценной и перспективной, а затем перейдем к рассмотрению вариантов ее реализации у различных производителей.

Недостающее звено

То, что виртуализация несет массу преимуществ для вычислительной инфраструктуры, убеждать никого не надо. Здесь и повышение степени использования («утилизации») оборудования, и улучшение управляемости, и лучшая защищенность данных. Например, благодаря виртуализации Facebook удалось добиться того, что на каждые 20-25 тыс. собственных серверов компании приходится всего один системный администратор. Но если вычислительные узлы и СХД уже давно и успешно виртуализированы, то с сетями передачи данных ситуация иная, что в известной степени сдерживает развитие отрасли дата-центров. Хотя технология «виртуального Ethernet» используется довольно давно, однако она способна объединить в условную сеть лишь виртуальные машины внутри одной вычислительной системы — в лучшем случае одного ЦОД.

В то же время активное развитие индустрии дата-центров и внедрение «облачных» технологий требует, чтобы виртуализация коснулась всей физической территориально распределенной сетевой инфраструктуры. Независимо от того, где, в каком дата-центре размещен сетевой узел, он должен быть доступен для управления, оптимизации и настройки так, будто бы находится в соседней комнате. Такой подход, разумеется, нужен не всем. По крайней мере, сейчас.

Основные потенциальные покупатели SDN-решений в их нынешнем виде — это крупные распределенные дата-центры и организации с развитой филиальной структурой (корпорации, госорганы). Для виртуализации сетевых функций существует также технология NVF (Network Functions Virtualization), которая развивается параллельно с SDN. Но поскольку она предназначена в первую очередь для операторов связи и сервис-провайдеров, в этой статье мы не будем ее рассматривать, сконцентрировавшись на решениях для ЦОД. В то же время именно в симбиозе SDN и NFV многие специалисты видят будущее крупных сетевых инфраструктур. Но пока что дело не идет дальше концептуальных обсуждений, не говоря уже о реализациях.

В контексте основной темы статьи стоит напомнить, что ключевым принципом SDN является физическое и логическое разделение уровней управления (Control Plane) и передачи данных (Data Plane или Forwarding Plane). В нынешних условиях оба они в том или ином виде содержатся в каждом сетевом устройстве корпоративного уровня. Применение SDN предполагает нали-

чие центрального аппаратно-программного элемента — «умного» контроллера, в котором содержится вся информация о топологии и настройках сети. К этому контроллеру прямо или опосредовано подключаются «рядовые» коммутаторы (а к ним — любые пользовательские устройства), не содержащие ничего кроме физических портов и средств для поддержания самых базовых функций, достаточных для удаленного централизованного администрирования (**рис. 1**).

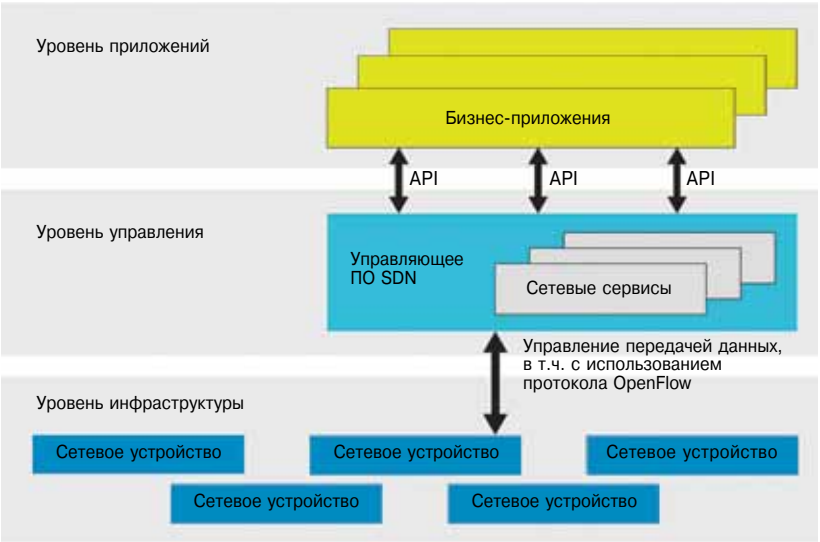

Рис. 1. Логическая схема SDN-сети

В современных крупных корпоративных сетях каждое устройство и каждый сегмент имеют массу индивидуальных настроек, работа с которыми усложняется по мере роста инфраструктуры — на каждой крупной площадке должен быть свой администратор. В случае SDN все управление может быть сведено в единый центр. Технология на базе протокола OpenFlow позволяет администратору видеть всю структуру сети и централизованно обновлять прошивки подключенных устройств (которых могут быть сотни или даже тысячи), задавая для каждого из них требуемые параметры, политики безопасности, предпочтительные маршруты передачи данных, параметры QoS и много чего другого. Основную работу здесь выполняет специализированное ПО. По сути, оно и является контроллером, аппаратная часть которого может быть представлена сервером или специальным коммутатором. Из-за своей программной сущности возможности SDN-сети, по сути, ограничены только фантазией разработчиков и деловой целесообразностью.

Контроллер может централизовано работать как с отдельными устройствами, так и с целыми группами. Ввиду отсутствия «интеллекта» у рядовых сетевых узлов, каждый из них может быть легко перемещен или заменен в случае поломки, чего нельзя сказать о самом контроллере, который является важнейшим, но и самым уязвимым элементом SDN-сети. Долгое время не удавалось реализовать его полноценное резервирование. Но в последних разработках эта проблема так или иначе решена у многих производителей. Например, данные о настройках сети копируются на съемный носитель или СХД, а оттуда в случае необходимости записываются на запасной контроллер, который находится в режиме ожидания — это один из вариантов.

В целом концепция SDN дополняет виртуализацией классическую триаду — серверы-СХД-сеть — и позволяет выйти на совершенно новый уровень — программно-конфигурируемый ЦОД (Software Define Data Center, SDDC). Концептуально идея выглядит вполне логично: вынести уровень управления и распределения всех ресурсов ЦОД на внешний аппаратный сервер, благо сегодня широко распространенные x86-системы обладают высокой вычислительной мощностью при относительно низкой цене. В любом случае привязка к «железу» не должна быть основной идеей, главное — это специализированное программное обеспечение. Но SDDC пока существует фактически лишь «на бумаге» да в головах идеологов.

Что касается совместимости решений SDN, то по идее продукты любых производителей должны легко сочетаться между собой, но этого еще не произошло. В каждом отдельном случае вопрос совместимости решается отдельно. На сегодняшний день собственные разработки в сфере программно-конфигурируемых сетей (так, примерно, переводится термин Software Define Network) предлагают ***Allied Telesis***, ***Avaya***, ***Brocade***, ***Cisco***, ***Dell***, ***Enterasys***, ***Extreme Networks***, ***IBM***, ***Hewlett-Packard***, ***Juniper***, ***NEC*** и другие. Например, в РФ собственный SDN-контроллер (очевидно, разработанный на базе решения ***Intel***) был выпущен Центром прикладных исследований компьютерных сетей в ноябре текущего года.

Следует отметить, что поскольку тема SDN еще достаточно свежая (первые рабочие компоненты появились на рынке не ранее 2008 года, и только с 2012-го о технологии заговорили как о более-менее целостном решении), с проектами в мире еще достаточно туго. Поэтому во многих случаях невозможно

проверить, насколько жизнеспособны и вообще реальны решения той или иной компании. Заявления «у нас есть SDN» можно услышать почти ото всех известных сетевых производителей, но что на самом деле за ними скрывается, иногда понять довольно сложно. Сведения по некоторым производителям весьма фрагментарны, и четкое представление об их концепции сформировать трудно. Особенно это касается тех вендоров, которые не имеют офисов (или представителей) в Украине ввиду отсутствия возможности лично пообщаться со специалистами. Поэтому в статье собраны основные сведения о решениях компаний, хорошо представленных на отечественном рынке.

Hewlett-Packard

На концепцию программно-конфигурируемых сетей HP возлагает довольно большие надежды. Компания является одним из крупнейших идеологов продвижения технологии на массовый рынок, предлагая целую серию разнообразных решений, объединенных в рамках общей концепции Virtual Application Networks (VAN). Подход предполагает наличие трех основных составляющих: инфраструктуры (Infrastructure), управления (Control) и приложений (Applications).

Основой системы является модуль Control, который представлен центральным контроллером, обеспечивающим абстрактное отображение инфраструктуры и отвечающим за выполнения политик, заданных администратором. Этот «узел» может быть как чисто программным (тогда он устанавливается на обычном x86-сервере), так и программно-аппаратным (выполненным на базе специального устройства). Контроллер поддерживает ряд основных функций, в т.ч. возможности сетевой виртуализации, безопасности, управления трафиком и т.д. Для взаимодействия с внешними SDN-приложениями имеется фирменный интерфейс RESTful. Кроме того, SDN-контроллер HP интегрируется с открытыми «облачными» платформами OpenStack и CloudStack.

Слой инфраструктуры — это физические и виртуальные сетевые устройства с поддержкой протокола OpenFlow и возможностью программируемого доступа со стороны контроллера. Таковых в продуктовом наборе HP уже десятки моделей (**рис. 2**).

На уровне приложений осуществляется выбор оптимального пути передачи данных, оптимизация производительности, обеспечение безопасности, QoS и т.д. Здесь HP предлагает комплексное ПО Virtual Cloud Networks (VCN), предназначенное для автоматизации работы с виртуальными сетями в «облачных» дата-центрах, а также систему обеспечения безопасности сетевого трафика Network

Рис. 2. Коммутатор HP Networking 5400Rzl2 с поддержкой OpenFlow

Protector. Последняя разработка для своевременного выявления угроз использует динамическую «облачную» репутационную базу данных HP TippingPoint DVLab (в которой, например, есть данные о более чем 1 млн. ботнетов) и может быть интегрирована с платформой ArcSight для анализа тревог. Кроме того, HP предлагает модуль Network Optimizer для автоматической балансировки нагрузки в SDN-сетях. В частности, уже отработан вариант оптимизации работы приложения для унифицированных коммуникаций MS Lync на SDN-сети, созданной с помощью решений HP.

Кстати, совсем недавно (в сентябре 2014 года) HP решила продвигать свои приложения для SDN в том числе через собственный онлайн-магазин. На момент запуска там будет предлагаться два приложения, собственно HP (Network Protector и Network Optimiser), а также шесть партнерских разработок, созданных компаниями Kemp, F5 и BlueCat.

Allied Telesis, Juniper и другие

Японская компания ***Allied Telesis*** также предлагает собственное решение для создания SDN. Его основа — фирменный протокол Allied Telesis Management Framework (AMF), который является элементом более общей концепции Virtual Core Fabric (VCF). Аппаратной основой для построения сетей VCF на базе AMF является семейство коммутаторов серии «x» (всего более сорока моделей). Концепция предполагает три уровня: ядро, распределение и доступ. На первом располагаются контроллеры SDN (AMF Masters), представленные шассийными коммутаторами SwitchBlade — x8112 (**рис. 3**) или x908, которые могут быть продублированы.

Уровни распределения, агрегации и доступа возложены на устройства серий x900, x610, x510, x210 (AMF Members). Платформа AMF позволяет автоматизировать многие сетевые функции, в числе которых — установка нового оборудования (в т.ч. после замены вышедшего из строя), резервное копирование данных контроллеров, создание VLAN и т.д.

Свои разработки для SDN ***Juniper*** позиционирует не только для использования в ЦОД, но

Рис. 3. Шассийные коммутаторы Allied Telesis SwitchBlade x8112 могут выступать в роли SDN-контроллеров

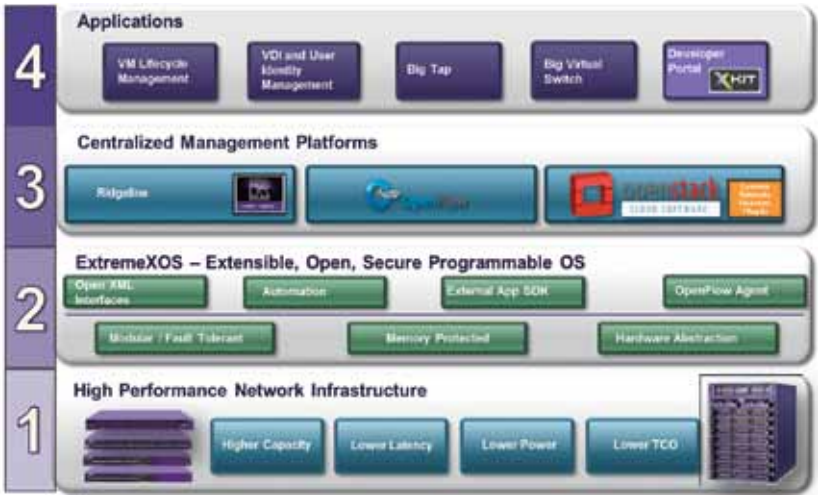

Рис. 4. Концептуальная схема SDN-решения компании Extreme Networks

и для MPLS-ядра в рамках единой операторской сетевой инфраструктуры. Аппаратной основой решений производителя являются маршрутизаторы 3D Universal Edge серии MX (на базе фирменной ОС JunOS и набора микросхем Junos Trio). Их подсистема JunosV App Engine обеспечивает виртуализацию сетевых служб под управлением платформы Junos Space Network Management. Также технологию SDN поддерживают коммутаторы серий EX и QFX, способные работать с различными открытыми и программируемыми интерфейсами. Устройства серии MX поддерживают протоколы OpenFlow и PCEP, коммутаторы QFX — OpenFlow. На всех платформах имеется инструментарий для управления конфигурациями.

Однако главным элементом системы можно назвать программную платформу Contrail — виртуальный централизованный контроллер программно-конфигурируемой сети. Кроме того, Juniper разработал специальный контроллер PCE, предназначенный для работы в MPLS-сетях, а также решение CloudCPE, предоставляющее инструменты работы в составе «облачных» сред операторов связи. Отличительной особенностью серии решений Juniper для SDN является наличие фирменного межсетевого экрана Firefly, оснащенного функциями NAT/FW/IPS. Второй многообещающий продукт — виртуальный маршрутизатор MX (vMX). В ближайшей перспективе планируется реализовать интеграцию vMX и Contrail. Отметим, что аппаратный маршрутизатор Juniper MX может интегрироваться с виртуальным контроллером Contrail по протоколу BGP.

Компания ***Extreme Networks*** также развивает направление SDN, предлагая на рынок собственный контроллер OneController, созданный на базе открытой программной платформы OpenDaylight, и фирменную технологию CoreFlow (**рис. 4**).

Кроме того, производитель предлагает специальный комплекс OneFabric Control Center, включающий в себя системы мониторинга и управления (NetSight, Data Center Manager, Mobile IAM), безопасности (NAC, IAM, IEM), а также глубокого анализа потоков данных (Purview). Поддерживаются различные модели проводного и беспроводного оборудования, на котором реализован протокол OpenFlow, под общим управлением операционной системы ExtremeXOS. Кроме того, имеется специальный программный инструментарий для разработки интерфейсов — OneFabric Connect SDN API.

Что касается ***Dell***, то это относительно новый игрок на сетевом рынке. Но активные приобретения отраслевых компаний позволили занять ей определенное место в этом сегменте. В отличие от многих конкурентов, Dell не имеет за собой шлейфа из устаревших технологий, которые необходимо поддерживать по тем или иным причинам (например, по условиям крупных контрактов). Вместо этого компания концентрируется на последних тенденциях сетевого рынка, в частности, предлагая разработки для SDN. Портфель решений в этом направлении включает в себя три основных компонента — ПО Active Fabric Controller, систему управления Active Fabric Manager и модульные коммутаторы Dell Networking S5000. Кроме того, в мае 2014 года Dell заключила партнерское соглашение о совместном продвижении SDN-решений с одним из пионеров этой отрасли — Big Switch Networks. Согласно условиям договора, заказчики, приобретающие Ethernet-коммутаторы Dell Networking S4810 и S6000, смогут использовать решения Big Switch Networks — операционную систему Switch Light OS и ПО для сетевого мониторинга Big Tap Monitoring Fabric.

Cisco: особое мнение

Решения Cisco стоят особняком от разработок других компаний, поскольку производитель реализует здесь собственный подход. Конечно Cisco, оставаясь в мировом тренде, поддерживает

«классический» SDN на базе протокола OpenFlow (более того, входит в Open Networking Foundation — неприбыльную организацию, занимающуюся развитием упомянутого открытого протокола). Но в отличие от всех перечисленных в статье производителей, продвигает и собственную независимую технологию программно-конфигурируемой сетевой инфраструктуры — Open Network Environment (которая является частью более общей концепции ACI). Дело в том, что по мнению представителей Cisco, нынешние реализации SDN все еще довольно «сырые», но сама идея программно-конфгурируемой сети здравая и перспективная. Платформа ONE включает в себя три основных компонента: контроллер и агенты, программные интерфейсы (Platform & ApplicaIon API), виртуальные сетевые функции. В отличие от «чистого» SDN, при котором имеются центральный контроллер и группа «рядовых» коммутаторов без встроенного «интеллекта», Cisco предлагает использовать нынешнюю аппаратную схему с традиционными коммутаторами, на которые устанавливаются программные модули (агенты), реализующие преимущества программно-конфигурируемой концепции.

Роль SDN-агента в инфраструктуре ONE отведена программному компоненту операционных систем Cisco (IOS XE, XR, NX-OS), который называется OnePK (ONE Platform/Programmatic Kit). Что отличает технологию Cisco от «классического» SDN-подхода — это возможность создания постоянного циклического обмена информацией, в котором задействованы как сетевая инфраструктура, так и приложения — например, аналитические системы или средства мониторинга политик контроля доступа. Таким образом, вместо совсем иной сети (SDN) концепция Cisco подразумевает использование привычной сети с расширенными возможностями.

Что касается ACI (которая появилась в составе решений вендора после приобретения в прошлом году компании Insieme), то по определению Cisco, она представляет собой комплексную инфраструктуру, ориентированную на приложения, объединяющую программное и аппаратное обеспечение с системами управления на базе политик. При этом строить инфраструктуру ACI предлагается с помощью различных вариантов т.н. «стартовых комплектов» (Starter Bundles).

Например, один из таких наборов включает в себя отказоустойчивый кластер из трех контроллеров APIC, два фиксированных или модульных магистральных коммутатора (spine switches), восемь оптических портов 40G, а также два или четыре (в зависимости от выбранной конфигурации комплекта) периферийных коммутатора (leaf switches). Данный комплект может применяться также для масштабирования комплексных решений серии UCS (FlexPod, VBlock). Еще есть возможность использовать ACI вместе с межсетевыми экранами Cisco серии ASA. Кроме того, имеется целый ряд решений, в которых ACI сочетается с продуктами других производителей — Citrix NetScaler, Embrane, F5 Synthesis.

Концепция SDN и ее практическая реализация имеет целый ряд преимуществ. Многие компании-заказчики уже присматриваются к ней или даже пытаются внедрять. Но пока таких случаев немного. Как ожидается, более-менее значимые проекты начнут появляться уже в следующем году, до 2017 года большинство крупных компаний осознают превосходство SDN, а к 2030-му эта технология станет доминирующей в корпоративном сегменте. Но пока что программно-конфигурируемые сети наталкиваются на сильное противодействие со стороны крупнейших поставщиков традиционных решений, которые не намерены включаться в новую «гонку вооружений», тем более в том сегменте, где они не обладают подавляющим преимуществом.

Сейчас это большой сдерживающий фактор. Ведь для того чтобы ощутить преимущества SDN, все компоненты сети (или, по крайней мере, большинство из них) должны поддерживать программно-конфигурируемый подход, а для этого сеть надо модернизировать. Сразу и полностью менять всю инфраструктуру, естественно, никто не будет, за исключением разве что отчаянных энтузиастов. Скорее всего, процесс начнется с модернизации отдельных сегментов. Но и здесь SDN придется выдерживать острую конкуренцию с традиционными сетевыми продуктами, которые приносят мировым производителям огромные прибыли (и так просто они их не отдадут). С другой стороны, SDN может стать тем фактором, который позволит увеличить долю на рынке для компаний, занимающих второе, третье и последующие места по уровню продаж в сегменте сетевых решений. Это, в свою очередь, будет угрожать позиции лидера, который, очевидно, не захочет уступить.

В любом случае, SDN — следствие технологического прогресса, поэтому она или подобная технология рано или поздно завоюет рынок, но вот в каком виде и как скоро это произойдет, вопрос открытый...

За помощь в подготовке публикации автор выражает признательность компаниям Allied Telesis, Cisco, Dell, S&T Ukraine, «МУК», а также отдельная благодарность лично Родиону Ковальчуку (Hewlett-Packard).

Игорь КИРИЛЛОВ, СиБ