Неоднозначность SDN

Менять удаленно сетевые настройки — к дальней дороге.
Старая админская примета.

Введение

В это трудно поверить несведущему человеку, но в интернете до сих пор используются протоколы, рождение которых состоялось еще в 70-е года прошлого века, то есть во времена ничтожного (по современным меркам) объема и разнообразия передаваемых данных. С тех пор магистральные "килобайты" сменились на "гигабиты", а работающие поверх инфраструктуры сервисы по разнообразию превзошли любой восточный базар. И конца этому процессу не видно: согласно некоторым данным объемы трафика увеличатся в 12 раз между 2012 и 2018 годами. Не удивительно, что современная сетевая архитектура обещает стать чуть ли не главным препятствием для дальнейшего развития базирующихся поверх нее телекоммуникационных услуг.

Разумеется, сеть непрерывно претерпевает модернизацию на всех уровнях. С появлением инновационных задач и выявлением очередных проблем, к стеку TCP/IP добавляются все новые протоколы, усложняется начинка сетевого оборудования, меняется физически транспортная инфраструктура. Новые технологии расширяют возможности старых протоколов, но при этом заметно усложняют управление сетью. К тому же, разработчики не стремятся работать безвозмездно, и каждая новая реализация очередного сетевого наворота продукта обычно продается в составе "фирменного" программно-аппаратного комплекса, и да еще подчас с проприетарными (т.е. закрытыми) протоколами.

Короче говоря, пересмотр принципов построения сетей назрел сам собой, и уже достаточно давно.

Варианты решения

Наиболее очевидный следующий технологический шаг - виртуализация. То есть инфраструктура должна работать так, словно обычная физическая сеть, но выбор модели и даже месторасположение оборудования никого не волнуют становится менее критичным. Соответственно, настраивая виртуальную сеть, администратор может не знать ее состава и архитектуры. Немаловажно, что в этом случае на одном комплекте оборудования может быть развернуто несколько независимых и никак не пересекающихся сетей, которые могут даже “не подозревать” о существовании друг друга.

Одной из наиболее перспективных разработок считается технология SDN (не путать с CDN) - Software-Defined Networking или программно-конфигурируемая сеть (ПКС). Не за особо качественные решения, а скорее потому что похожа на Linux в отличие от проприетарных решений коммерческих компаний ведется на базе открытого протокола Open Flow.

Предыстория SDN, протокол OpenFlow

В 2007 г. специалисты из университетов Беркли и Стэнфорда, Мартин Касадо (Martin Casado), Ник МакКьоун (Nick McKeown) и Скотт Шенкер (Scott Shenker) организовали компанию Nicira, на базе которой началась разработка платформы в сфере виртуализации сетей (network virtualization platform, NPV). В июле 2012 года эта компания была куплена крупнейшим американским производителем программного обеспечения для виртуализации, компанией VMvare, за 1,26 млрд. долларов. Ник МакКьоун и Скотт Шенкер входят в технический и наблюдательный советы при российской организации, занимающейся вопросами разработки и развития ПКС - ЦПИКС.






Ник МакКьоун, Скотт Шенкер и Мартин Касадо

Суть концепции SDN заключается в разделении функций управления и пересылки данных, передаче функций маршрутизации контроллеру сети, и реализации на основе этого принципа легко масштабируемой, быстро и гибко настраиваемой виртуальной сети.

Разделение уровней управления (Control Plane) и коммутации (Forwarding plane) избавляет коммутаторы и маршрутизаторы от значительной доли вычислительной нагрузки. Все, что от них теперь требуется, это максимально быстро пересылать пакеты из одного порта в другой, согласно таблицы маршрутизации, поступающей извне от контроллера сети. Контроллер же, вместо построения маршрута для каждого пакета, как это предусмотрено в традиционной схеме, принимает решение однократно, а потом гонит все однотипные пакеты потоком по готовому маршруту, пока не изменится состояние сети или характер трафика. Справедливости ради, на "rocket science" это похоже мало - современное оборудование использует аналогичные методы по оптимизации потоков данных, хоть и на уровне конкретного узла, а не всей сети.

Основная идея в экономии другом: не имеет ни малейшего значения, кто именно произвел используемые устройства - лишь бы они поддерживали открытый протокол Open Flow. С определенной долей абстракции можно говорить, что вся сеть ПКС может быть построена на однотипных, не слишком сложных (а значит и недорогих) коммутаторах с Open Flow. Или даже вообще на любых устройствах с поддержкой OpenFlow, вне зависимости от производителя и назначения.

Контроллером же сети может выступать отдельный сервер или даже обычный компьютер администратора, на котором установлена сетевая операционная система, обеспечивающая интерфейсы управления между сетевыми приложениями и коммутаторами сети.

К настоящему времени создано уже больше трех десятков сетевых операционных систем, среди которых можно назвать NOX, POX, Beacon, Maestro, Trema, BigSwitch и FloodLight. Также следует отметить, что управление контроллерами сетей SDN также может быть подчинено одному общему контроллеру, что позволяет строить виртуальные сети каскадами с любым уровнем вложенности.

Следует отметить, что часто вместе с термином “SDN” соседствует еще одна аббревиатура - NFV (network-functions virtualization), т.е. виртуализация сетевых функций. SDN и NFV во многом похожи, имеют много одинаковых компонентов и преследуют решение близких задач, в число которых

входит упрощение сетей, снижение CAPEX и OPEX, обеспечение максимальной автоматизации управления сетями.

Применимость

Можно говорить о четырех основных областях применения SDN: коммутация, контроллеры, виртуализация облачных приложений и виртуализация средств безопасности сетевых решений. Отсюда следуют основные направления, где новая технология пытается найти свое место:

- ЦОДы,
- облачные технологии,
- сети провайдеров,
- корпоративные сети,
- локальные сети (домашние),
- безопасность.

До локальных сетей новая технология, видимо, доберется еще нескоро, но такая возможность предусматривается разработчиками. Например, для настройки локальных сетей с управлением трафиком внутри них, а также с возможностью предоставления операторами услуг по удаленной настройке таких сетей.

С корпоративными сетями ситуация веселее. Например, Google самостоятельно разработал OpenFlow-коммутаторы и перевел на SDN всю внутреннюю сеть G-Scale, предназначенную для обмена данными между собственными дата-центрами компании.

Кроме того, SDN-архитектура работает в реальной сети сотовой связи и может использоваться в mesh-сетях.

Преимущества ПКС

Перехват управления таблицами маршрутизации всех сетевых устройств и перенос расчета маршрутов из “мозгов” маршрутизатора на общий внешний контроллер влечет за собой множество самых разных последствий. И первым из них следует назвать тот факт, что старый девиз "Cisco is a software company" доводится до логического финала - любые задачи по управлению сетями переходят в ведение программистов, поскольку решаются написанием соответствующего кода. Что в теории позволяет быстро отвечать на любые неожиданные изменения в структуре и объемах трафика. Например, обеспечивает администратору возможность изменить конфигурацию сети в случае атаки извне, чтобы локализовать, изолировать или даже блокировать потоки вредоносного трафика, с какой стороны границы сети он бы не приходил.

В целом, после изучения всех “за” и “против”, остается впечатление, что изначальную ресурсную избыточность IP-сетей хитрые ПКС-ники решили использовать для получения прибавки в скорости передачи данных. Нисколько при этом не боясь потерять в надежности, поскольку отказоустойчивость самой инфраструктуры (как устройств, так и линий) за последние четверть века возросла многократно.

Неполный список ожидаемых преимуществ от внедрения ПКС, выглядит следующим образом:

- Конфигурация всей сети хранится в одном месте, на компьютере администратора (это преимущество является одновременно и недостатком);
- Вместо расчета маршрута для каждого пакета используется принцип потоков данных, в маршрутизацию которых не нужно вносить изменений - значит есть надежда, что они будут обрабатываться на максимально возможной скорости;
- Простое и дешевое оборудования - благодаря этому снижаются капитальные и операционные затраты (по некоторым данным, сокращение до 30%), упрощается обслуживание;
- Новые решения для бесшовного Wi-Fi-роуминга (например, проект OpenRoads);
- Полная загрузка простаивающих аппаратных мощностей, увеличение пропускной способности каналов за счет более рационального использования оборудования;
- Снижение эксплуатационных расходов;
- Простая реализация добавления нового функционала;
- Мобильность всех сетей, возможность их миграции;
- Возможность замены оборудования без остановки работы сети;
- Возможность проводить любые эксперименты на отдельной виртуальной сети, использующей оборудование, обслуживающее основную сеть, без опасности нарушить ее работу;
- Удобство управления всей сетью разом;
- Простота обеспечения мер безопасности и пресечения несанкционированного вторжения на сеть;

- Минимальная сходимость в случае появления сбойного участка на сети;
- Для приложений сеть выглядит единым логическим коммутатором;
- Возможность организации новых услуг, поскольку снимаются физические ограничения, накладываемые ограниченным числом производителей оборудования.

Таким образом, с точки зрения бизнеса, ведущим достоинством ПКС является снижение издержек за счет более интенсивного использования существующего оборудования, уменьшения капитальных затрат, связанных с более дешевыми устройствами, и операционных расходов, т.к. вся сеть находится под тотальным контролем из одной точки.

Но если вы такие умные, то почему строем не ходите? что, в таком случае, сдерживает стремительное распространение концепции ПКС?

Недостатки

Всю эту замечательную “бочку мёда” отравляет несколько “ложек” настолько ядрёного “дегтя”, что многие специалисты считают шумиху вокруг SDN очередным маркетинговым пузырём, призванным не столько решать проблемы сетей, сколько выкачивать средства из “кармана” оператора.

Разброс критических замечаний довольно широк: от сомнений, что скорость обработки данных можно увеличить такими средствами, до подозрений, что как раз централизация управления сетью может стать настоящей головной болью. Ведь IP-сети изначально разрабатывались как отказоустойчивое решение, способное работать даже при уничтожении отдельных узлов и линий связи. Современный интернет не требует функционирования в условиях ковровой ядерной бомбежки во всяком случае пока, однако человека с экскаватором в неумелых руках пока никто не отменял.

Разумеется, у сторонников ПКС есть контраргументы, которые также подвергаются критике, с дальнейшим переходом любого диалога на эту тему в режим Intel vs AMD малоконструктивного спора.

Итак, основные подозрения осторожных специалистов:

- В случае отсутствия связи между контроллером и устройствами сети, коммутаторы переходят в дефолтное состояние и мгновенно превращаются в неуправляемую структуру. Или и вовсе в структуру неработающую, если какие-либо ее настройки требовали постоянной работы контроллера.
- Ошибка в программировании контроллера (а человеческий фактор никто не отменял) приведет к серьезным проблемам на всей сети, которую он обслуживает.
- Контроллер становится основной уязвимой точкой и главной целью для атак со стороны злоумышленников.
- Интересная ситуация может получиться в тех сетях, где будет использоваться оборудование, поддерживающее OpenFlow (а такого оборудования становится все больше), притом, что эта поддержка будет отключена за ненадобностью. По всей видимости, владельцам таких сетей придется следить за тем, чтобы однажды поддержка OpenFlow не оказалось вдруг каким-то образом включенной, а устройства не были вовлечены в работу чужой сети.
- Пока такого рода управление (вынесенное в отдельный control plane, либо по-старинке в ядре операционной системы) делается проприетарным софтом, существуют понятия «ответственность», «техническая поддержка», «SLA» и т.п. А если этим занимается нечто такое, к чему вендор не имеет отношения (кроме API), то кому конечный пользователь станет предъявлять претензии? Кто станет гарантировать работу сложнейшей структуры, собранной на базе “открытого” софта и простых коммутаторов?

Отечественный SDN

Среди осинок и березок На Родине слонов В России тема ПКС также не оставлена без внимания. Работа в этом направлении входит в список приоритетных научных задач, сформулированных правительством и утвержденных президентом Российской Федерации.

Из наиболее крупных отечественных компаний, Ростелеком с 2012 года активно изучает возможности ПКС, а в мае текущего года заявил о начале внедрений технологий SDN и NFV (виртуализация сетевых функций).

Работают над ПКС и отечественные ученые. Например, существует Центр прикладных исследований компьютерных сетей (ЦПИКС) (фактически, начал работать в мае 2012 года). Инициатор проекта – венчурный инвестор Александр Галицкий. Руководит организацией Руслан Смелянский.

Заявленные направления исследований Центра выглядят следующим образом:

- Разработка ПКС-моделей, методов, технологий и решений-прототипов;

- Экспериментальное подтверждение заявленных характеристик Open Flow,
- Создание математических моделей и обоснование методов, используемых для разработки приложений в ПКС-сетях;
- Создание инструментальных средств для разработки и отладки приложений для работы в ПКС сетях;
- Разработка прототипа сетевой операционной системы с открытым кодом для управления ПКС сетями;
- Разработка методов и средств стыковки ПКС-сетей с сетями традиционной архитектуры;
- Разработка прототипа Open Flow-коммутатора с оптимизированной архитектурой;
- Разработка методов и средств обеспечения безопасности ПКС-сетей.

В феврале 2013 года ЦПИКС выиграл грант Министерства образования и науки РФ на создание и развитие отечественной платформы с открытым программным кодом для управления программно-конфигурируемыми сетями (ПКС), а в июне 2014 года провел пилотное испытание прототипа первого универсального Wi-Fi контроллера для сетей ПКС, “Chandelle”. Возможности нового решения были продемонстрированы при организации гостевого Wi-Fi-доступа для девяти тысяч участников Startup Village в Сколково (интересно, как оно работало на самом деле?)

Прогнозы небывалых прибылей

Если технические прогнозы касательно дальнейшей судьбы SDN решаются делать единицы специалистов, то задержек с финансовыми прорицаниями - нет, и не предвидится.

Грядущие шкуры неубитых медведей доходы от рынка услуг, связанных с технологией SDN, с удовольствием считают как отдельные финансисты, так и всевозможные бухгалтерские конторы консалтинговые компании.

Например:

- Венчурный фонд Andressen Horowitz заявляет о том, что рынок ПКС-решений через несколько лет будет составлять около 40-50 млрд. долларов.
- Аналитическое агентство Markets&Markets в 2012 году предположило, что объем рынка ПКС-продуктов к 2016 г. будет превышать 2 млрд. долларов.
- Аналитик Кейси Куиллин из агентства Dell'Oro Group предполагает, что в период с 2010 до 2016 год общая сумма расходов компаний на ПКС и OpenFlow возрастут более чем в 17 раз.
- В апреле 2013 г. появился еще один прогноз развития рынка ПКС-решений, подготовленный информационным агентством SDNCentral, компанией Plexxi и венчурным фондом Lightspeed Ventures. Согласно этому отчету, объем рынка ПКС-решений к 2018 г. может преодолеть сумму в 35 млрд. долларов.
- По прогнозам SDNCentral, мировой рынок SDN составил в 2013 г. 1,5 млрд. долларов, а к 2018 г. достигнет 35,6 млрд. долларов. Фактически, речь идет о росте в 24 (!) раза. При этом к концу прогнозного периода около 40% всех расходов на сети передачи данных будут связаны с SDN.
- По прогнозам Research and Markets, в 2012-2016 гг. среднегодовой прирост глобального рынка программно-управляемых сетей составит 151%.

Стартапы ПКС

Как и в большинстве затей, опирающихся на высокотехнологичные разработки, большие надежды возлагаются на стартапы. Уже упоминавшаяся компания Nicira, была лишь одним из десятков стартапов, взявшихся за разработку SDN-технологий, и попавших в центр внимания прессы, благодаря громким приобретениям крупными производителями или другим финансовым достижениям.

Например:

- Big Switch основан в 2010 году, собрал 50 млн. долларов венчурных инвестиций.
- Vyatta - компания создана в Калифорнии в 2005 году. Разрабатывала решения для маршрутизации на базе открытой платформы Vyatta Network OS. Успела похвастаться более чем тысячей клиентов, и более, чем миллионом загрузок OS. Позиционировала себя, как конкурента Cisco. Куплена в 2012 году разработчиком оборудования для дата-центров, компанией Brocade.
- Contrail Systems. Стартап создан в 2012 году. Один из основателей - бывший тех.директор Juniper, Кирити Компелла. Велась разработка стандартных решений по управлению виртуальными сетями и их интеграции с другими платформами. Через два дня после выхода на рынок в декабре 2012 года куплен Juniper за 176 млн. долларов.
- Стартап Xsigo был куплен компанией Oracle.
- Компанию Insieme Networks - купила Cisco. Она же, в ноябре 2012 года купила компанию Carriden за 141 млн. долларов.

- Присоединился к этому тренду и Ростелеком. В августе текущего года представителями отечественного гиганта было заявлено о поиске стартапов-разработчиков SDN- и NFV-решений.

Вендоры

А что же производители оборудования? Ведь недаром же тратятся миллионы и миллиарды зеленых рублей долларов на покупку стартапов, а точнее - технологий и специалистов? Казалось бы, зачем крупному вендору вкладываться в “открытые” технологии, подрывающие интерес к его собственным, проприетарным и уникальным, протоколам и системам?

Дело, по всей видимости, в том, что само понятие ПКС - лишь общая концепция, конкретная реализация которой может значительно отличаться в зависимости от разработчика. Поэтому имеется возможность, не отказываясь от модной и многообещающей, хоть и “открытой” технологии, создать такие устройства и ПО, которые по-прежнему будут позиционироваться компаниями, как уникальная, и отчасти “закрытая”, разработка.

В этом случае, поддержка протокола Open Flow становится “общим знаменателем”, который обеспечит совместимость сетевых устройств от разных производителей, но контроллер сети, скорее всего, будет “заточен” для работы со “своим железом”. И тогда, использование на сети оборудование одного вендора, будет хоть и необязательным, но весьма желательным фактором.

Даже беглый поиск позволяет легко обнаружить, что устройства с поддержкой OpenFlow, выпускаемые в рамках концепции ПКС, не только вовсю выпускаются главными производителями сетевого железа планеты, но и давно имеются в продаже. Без претензий на всеохватность, перечислим наиболее крупных игроков рынка, плотно занимающихся разработками в рамках концепции SDN.

- Cisco подошла к вопросу предельно серьезно и основательно с концепцией Cisco ONE. Каждое устройство имеет свой control plane, но при этом позволяет манипулировать отдельными потоками с удаленного контроллера. Коммутаторы Nexus и Catalyst 35xx могут работать как в обычных, так и в SDN-сетях.
- Juniper добавила поддержку OpenFlow в JunOS SDK, а позже объявила о реализации этой технологии в коммутаторах серий EX и MX (например, EX4600-40F).
- Альянс Virtual Computing Environment, организованный Cisco, EMC и VMware, представил в феврале версию платформы виртуализации vBlock, ориентированную на ЦОДы среднего и малого размера.
- IBM выпустила контроллер сети в виде софта на базе Linux. Компания Avaya анонсировала фреймворк для своих программно-определяемых дата-центров (Software-Defined Data Center). В HP идет работа над стратегией HP Virtual Application Networks.
- Brocade выпустила коммутатор VDX 8770. Реализация SDN возможна в Agile-коммутаторах Huawei S12700. Не отстает от конкурентов и Dell.
- NEC выпустила распределенный виртуальный коммутатор ProgrammableFlow 1000 стандарта OpenFlow, поддерживающий Hyper-V в Windows Server 2012.
- Alcatel-Lucent объявила о новой стратегии Application Fluent Network: добавление SDN-функциональности в существующие коммутаторы OmniSwitch.
- Hewlett-Packard реализовала поддержку SDN/OpenFlow уже в десятках своих коммутаторов, а в перспективе все они будут работать в единой сетевой архитектуре FlexNetwork.
- Давно торгуют своими OpenFlow-коммутаторами Extreme (Summit X670V-48x) и “НАГ” (SNR-S4550-24XQ-AC).

Примечательные факты

Напоследок, хотелось бы озвучить несколько примечательных фактов, так или иначе, имеющих отношение к SDN.

- Huawei и 21Vianet запустили крупнейшую в Китае коммерческую сеть SDN.
- В 2009 году технологии программно-конфигурируемых сетей появились в списке 10 быстрорастущих технологий, ежегодно составляемом MIT Technology Review, после чего стали (наряду с протоколом Openflow) объектом пристального внимания не только в академических исследованиях, но и со стороны коммерческого сектора.
- Большая и открытая 100-Gigabit Ethernet сеть на основе протокола OpenFlow под названием Innovation Platform, реализуется в таком глобальном проекте, как Internet 2.
- На конференции российских операторов связи КРОС-2014, звучали доклады, посвященные в той или иной степени, концепции SDN, от таких производителей оборудования, как BTI и Ericsson.

А что об этом думают операторы?

Мы задали один единственный вопрос о планах, связанных с SDN, нескольким альтернативным

операторам связи. И получили на него очень разные, но, в то же время, симптоматично-похожие ответы.

Вопрос: Планирует ли ваша компания в обозримом будущем использовать какие-либо элементы концепции SDN (в частности, коммутаторы с поддержкой OpenFlow), и почему?

Эдуард Афонцев, директор «Дом.ru» (Екатеринбург):

> Давно изучаем SDN и опыт их применения, в настоящее время активно тестируем. В продакшн пока вводить не планируем - по крайней мере, до тех пор, пока не проведем все тесты, и не убедимся в абсолютной надежности технологии.

Леонид Скрипка, директор по информационным технологиям компании SevStar (Севастополь):

> Наша компания не планирует использовать данную технологию. Причины:
>
> 1. Необходимость замены практически всего оборудования.
> 2. В случае перехода на новую технологию, нам потребуется значительная переделка нашей системы управления, хотя на текущий момент нас устраивает то, что у нас есть.
> 3. Заявленное преимущество технологии - "Снижение стоимости оборудования за счет его упрощения" - к сожалению, на деле не является таковым. Оборудование получается дороже, так как поддержка OpenFlow преподносится производителями как дополнительный функционал. Также, оборудование, которое поддерживает OpenFlow, выпускается не самыми дешевыми вендорами (Extreme, Cisco, Brocade). Как следствие, общее решение дешевле не получается.
> 4. Необходимость покупки контроллера, а лучше двух (один - резервный) приводит опять же к удорожанию системы в целом.
>
> Ну, если по пунктам 3 и 4 еще можно поспорить и возможно это мое субъективное мнение (если честно, глубоко не исследовал эту тему:)), то с пунктами 1 и 2 бороться очень тяжело.

Артем Зубков, директор компании КСТ (Симферополь):

> А у нас всего 10 тыс клиентов , работает пара mx80 и Extreme 670 - вот и все железки. А так, в теории, sdn очень интересная концепция, и я бы с удовольствием начал внедрять какие-то элементы. Сама по себе, это замечательная идея - "сеть без админа".

Горбунов Андрей, технический директор ООО "Сити-Телеком" (Армавир):

> Технологии SDN предназначены, в первую очередь, для дата-центров. Мы, как оператор FTTB, не видим каких-либо плюсов в данных решениях для себя. Топология сети используется максимально простая. Наш абонент физически привязан к узлу кабелем и не может оказаться внезапно в другом районе. К тому же, точка подключения явно указана в договоре.

Антон Воронин, заместитель технического директора компании "Интерсвязь" (Челябинск):

> Технология SDN перспективна и интересна с точки зрения удобства управления крупными разветвлёнными сетями. В проводных сетях масштаба города она будет наиболее востребована. Однако этой технологией пока не оснащается тот класс оборудования, который массово используется операторами связи в городских сетях. Но мы думаем, что и это дело ближайшего будущего.
>
> А пока мы (и наверняка, не только мы) решаем вопросы управляемости и конфигурируемости большой разветвлённой сети, создавая собственные автоматизированные средства. Ручное управление в таких масштабах перестало быть возможным уже давно.

Выводы

Если передать смысл "правильными словами", то современные технологии действительно могут стать ограничивающим фактором для развития глобальной сети и сетевых сервисов, но за прошедшее время отработаны за годы до такого состояния, что функционируют достаточно надежно. Так что полный переход "на SDN" не может рассматриваться всерьез. Поэтому необходима разработка гибридных решений, которые и помогут начать глобальный переход к программно-конфигурируемым сетям. Говоря проще, сдвинуть с места наработанные за 40 лет решения - задача из области фантастики. Но попытаться занять какие-то локальные ниши можно уже сейчас.

Что касается предположений, некоторых сторонников SDN о мощном давлении, которое почувствуют

на себе производители железа из-за открытости протокола OpenFlow, то выглядят они пока, мягко говоря, несерьезно. Да, в теории SDN имеет огромные перспективы. И над тем, чтобы эти перспективы воплотились в жизнь, работают десятки тысяч специалистов по всему миру. Жаль только жить в эту пору прекрасную… Но говорить о светлом будущем с SDN, в которое мы вот-вот вступим, как минимум, преждевременно. И будет оставаться преждевременным еще не один год.