Internet Engineering Task Force (IETF)
Request for Comments: 7149
Category: Informational
ISSN: 2070-1721

M. Boucadair
C. Jacquenet
France Telecom

March 2014

Программно-определяемые сети с точки зрения сервис-провайдеров

Software-Defined Networking: A Perspective from within a Service Provider Environment

Тезисы

Программно-определяемые сети (SDN[1]) в течение нескольких последних лет были одним из наиболее обсуждаемых вопросов в сетевой индустрии. Тем не менее четкого и общепринятого определения SDN до сих пор не дано. Этот документ пытается описать «ландшафт» SDN, указав требования, проблемы и другие связанные с SDN вопросы с точки зрения поставщиков сетевых услуг.

Это не бесконечные обсуждения, что же такое SDN, а скорее попытка предложить функциональную систематику методов, которые могут применяться «под зонтиком» SDN, и предложить варианты решения «подвешенных» вопросов, связанных с комбинированным применением таких методов. Определение SDN упомянуто лишь для ясности.

Статус документа

Этот документ не является спецификацией стандарта Internet и публикуется с информационными целями.

Документ является результатом работы IETF[2] и представляет согласованное мнение сообщества IETF. Документ был вынесен на открытое обсуждение и одобрен для публикации IESG[3]. Не все документы, одобренные IESG, претендуют на статус стандарта Internet (см. раздел 2 документа RFC 5741).

Информация о статусе этого документа, обнаруженных ошибках и способах обратной связи доступна по ссылке http://www.rfc-editor.org/info/rfc7149.

Оглавление

1. Введение

Сеть Internet стала сетевой федерацией, поддерживающей широкий спектр предлагаемых услуг. Предоставление услуг типа IP VPN предполагает совместную активацию различных возможностей, которые включают (но не обязательно ограничиваются) пересылку и маршрутизацию (управление схемами адресации заказчиков, динамический расчет пути для набора префиксов адресатов, динамическая организация туннелей и т. п.), управление качеством

[1]Software-Defined Networking.
[2]Internet Engineering Task Force.
[3]Internet Engineering Steering Group.

обслуживания (например, классификация, маркировка, кондиционирование и планирование трафика), обеспечение безопасности (фильтрация для защиты сайтов заказчиков от атак из сети, предотвращение создания ошибочных маршрутов и т. п.) и поддержку (например, обнаружение и обработка отказов).

Поскольку растет не только разнообразие, но и сложность услуг, их устройство, доставка и работа также стали сложной алхимией, зачастую требующей различных навыков. Эта ситуация усугубляется ростом числа (сетевых) протоколов и инструментов, а также современными тенденциями сближения ATAWAD[1], когда конечный пользователь может получать широкий спектр услуг, на которые он подписан, независимо от технологии доступа и устройства - где бы этот пользователь ни подключился к сети, даже если он находится в движении.

Тем не менее, большинство таких услуг было развернуто в последнее десятилетие прежде всего на базе статических процедур предоставления услуг, которые все сильнее подвержены риску ввода ошибочных команд настройки конфигурации. Кроме того, большинство таких услуг не предполагает какого-либо специфического согласования между заказчиком и поставщиком услуг сверх обычных финансовых соглашений.

В лучшем случае пятилетние генеральные планы задают политику планирования сети, которая будет выполняться сервис-провайдером с учетом предполагаемых перспектив развития бизнеса, рассчитанных вручную предсказаний трафика и сближения рынков (фиксированный - мобильный, домашний - корпоративный). Такая политика планирования сети может существенно повлиять на распределение ресурсов в сети, но она явно не позволит адекватно реагировать на динамичные запросы заказчиков в стиле «всегда на связи». Потребность в улучшенных процедурах предоставления услуг (включая время, требуемое для доставки после заключения соглашения) для корпоративных заказчиков еще более важна.

Кроме того, для управления применяются разные инструменты, порой ориентированные на конкретный сервис, но их применение не всегда координируется с целями агрегирования, сопоставления и обработки событий. Недостаток координации может приводить к усложнению систем и снижению качества.

Поэтому мультисервисные, мультипротокольные сети на основе множества конвергентных технологий с динамической адаптацией в ближайшем будущем станут одной из основных проблем сервис-провайдеров.

В этом документе предпринята попытка прояснить сферу применения SDN на основе функциональной систематики методов, которые могут применяться в SDN, с точки зрения поставщиков услуг.

2. Введение SDN

2.1. Тавтология?

Разделение уровней пересылки и управления (помимо вопросов, связанных с реализацией) стало практически уловкой для продвижения гибкости как ключевого свойства модели SDN. Технически большинство маршрутизаторов используют такое разделение уже в течение десятилетий. Процессы маршрутизации (такие как расчет маршрутов IGP и BGP) зачастую выполняются на программном уровне, а функции пересылки обычно реализуются аппаратно.

Таким образом, на момент написания этого документа слова о разделении уровней представляются скорей тавтологией, нежели чем-то новым.

Эффективность же централизованного, «встроенного в контроллер» уровня управления для оптимизации расчета маршрутов до заполнения базы FIB[2] является не вполне очевидной.

2.2. Гибкость

Пропагандисты SDN утверждают, что их подход обеспечивает дополнительную гибкость в работе сетей. Это, несомненно, является одной из основных целей, к которым стремятся сервис-провайдеры. Причина заключается в том, что способность динамически приспосабливаться к широкому спектру клиентских запросов для гибкого предоставления услуг является важным конкурентным преимуществом. Но гибкость - это не только разделение уровней управления и пересылки для упрощения процессов принятия решений.

Например, способность воспринять краткосрочную потребность клиента в дополнительной пропускной способности для просмотра потокового видео на устройстве является примером гибкости, которую реально хотят получить многие современные операторы.

В этом плане способность предсказать поведение сети в зависимости от предоставляемых услуг имеет решающее значение для сервис-провайдеров, чтобы они могли оценить влияние новых услуг, активизации дополнительных функций или применения данного набора (новых) правил с финансовой и технической стороны. Это говорит в пользу исследования усовершенствованных механизмов эмуляции сетей, например, [LS-DISTRIB].

С учетом довольно широкой области применения термина «гибкость» следует отметить приведенные ниже аспекты.

- Современные решения SDN считаются гибкими, хотя понятие гибкости вряд ли определено. Точные характеристики того, что в реальности означает гибкость, пока не заданы. Поэтому нужно продолжать работу по определению гибкости в свете различных критериев (например, способности развития сети в зависимости от сложностей, создаваемых интеграцией методов SDN, и возможностями эволюционного развития, т. е. постепенного внедрения устройств SDN без нарушения работы сети и сетевых услуг).
- Использование программируемых интерфейсов само по себе не является целью, скорее это средство облегчения процедур настройки для повышения уровня гибкости.

2.3. Предварительное определение

Мы определяем SDN как набор методов, используемых для облегчения проектирования, доставки и эксплуатации сетевых услуг детерминируемым, динамичным и расширяемым способом. Указанный детерминизм относится к способности полностью управлять различными компонентами цепочки предоставления услуг так, чтобы эти услуги соответствовали согласованным с потребителем условиям контракта.

Таким образом, детерминизм предполагает управление структурой сетевых услуг, их организацией и предоставлением, а также пересылкой трафика через сеть для оптимизации использования ресурсов. Хотя это явно не указано в документе, детерминизм лежит в основе любых действий, которые сервис-провайдер может предпринимать

[1]Any Time, Any Where, Any Device - всегда, везде и на любом устройстве.
[2]Forwarding Information Base - база данных для пересылки.

после согласования параметров услуги, от задач настройки параметров до предоставления услуги и обеспечения гарантий обслуживания (параграф 2.4).

Такое определение предполагает внедрение высокого уровня автоматизации процедур предоставления услуг и сетевых операций. Поскольку сетевое взаимодействие по своей природе управляется программным путем, приведенное выше определение не выделяет «программно-определяемых» свойств решений SDN.

2.4. Функциональные метадомены

Методы SDN можно классифицировать по перечисленным ниже функциональным метадоменам.

- Динамическое обнаружение сетевой топологии, устройств и их возможностей вместе с относящейся к этому информацией и моделями данных, которые точно описывают такую топологию, устройства и их возможности.
- Демонстрация сетевых услуг и их характеристик, а также динамическое согласование набора параметров сервиса, которые будут служить для измерения качества, связанного с предоставлением услуги или набора услуг. Примером может служить [CPP].
- Методы, применяемые системами динамического распределения ресурсов и схемами исполнения правил для соответствующего программирования сетей. Решения для динамического распределения ресурсов и применения правил обычно являются результатом сопоставления различных входных данных, таких как состояние доступных ресурсов сети в данный момент, число запросов абонентов на обслуживание, которые нужно обслужить в данное время, прогнозы трафика, возможная потребность в запуске дополнительных циклов предоставления ресурсов в соответствии с многолетним генеральным планом и т. п.
- Механизмы динамической обратной связи для оценки эффективности данной политики (или набора правил) с точки зрения предоставления услуг и обеспечения гарантий.

3. Реальность

Сетевая экосистема стала чрезвычайно сложной и требовательной с точки зрения отказоустойчивости, производительности, расширяемости, гибкости, эластичности и т. п. Это означает, в частности, что сервис-провайдеры и сетевые операторы должны иметь дело с такой сложностью и эксплуатировать сетевую инфраструктуру, которая может легко развиваться, сохранять расширяемость, гарантировать отказоустойчивость и доступность, а также быть устойчивой к атакам на отказ в обслуживании.

При внедрении новых сетевых функций на основе SDN, очевидно, следует принимать во внимание этот контекст, особенно с точки зрения его влияния на расходы.

3.1. Помним о прошлом

Методы SDN - это не следующий большой шаг вперед, а скорее пересмотр предложений, которые исследовались в течение нескольких лет, таких как активные или программируемые сети [AN] [PN]. Фактически, некоторые из объявленных «новыми» функций SDN уже были реализованы (например, NMS[1] и PCE[2] [RFC4655]) и поддерживаются производителями в течение достаточно долгого времени.

Некоторые из этих функций были стандартизованы (например, маршрутизация на основе DNS [RFC1383]), что можно считать иллюстрацией разделения уровней управления и пересылки или ForCES[3] [RFC5810] [RFC5812].

Кроме того, модель сетевого управления на основе правил [RFC2753], предложенная в начале 2000-х годов, была разработана для организации доступных ресурсов с помощью PDP[4], которые управляют расширенными возможностями автономного (offline) построения трафика. Эта модель может взаимодействовать с программными модулями, встроенными в управляемые устройства, по основному каналу (in-band).

PDP является точкой принятия решений в политике. PDP используют службу каталогов в качестве репозитория правил, хранящего информацию, которая может извлекаться и обновляться PDP. Точки PDP доставляют правила политики в точки исполнения правил PEP[5] в форме информации о реализации политики, включающей данные конфигурации.

В точках PEP исполняются решения политики. PEP встраиваются в (сетевые) устройства, которые динамически настраиваются на основе данных в формате политики, которые обрабатываются в PEP. Точки PEP запрашивают конфигурацию у PDP, сохраняя данные конфигурации в базе PIB[6] и делегируя принятие решений точкам PDP.

Методы SDN в целом являются примером модели управления сетью на основе правил. В этом контексте методы SDN можно применять для активации возможностей по запросу, динамического подключения ресурсов сети или хранилища, а также для управления адаптивными сетями по событиям (например, изменение топологии), триггерам (например, уведомление об отказе канала) и т. п.

3.2. Будем прагматичными

Подходы SDN должны быть целостными в глобальном и сетевом масштабе. Речь не идет о настройке устройств одного за другим для исполнения конкретной политики пересылки. Вместо этого методы SDN нацелены на настройку и работу целого ряда устройств в масштабе сети для автоматизированного предоставления услуг [AUTOMATION] от согласования (например, [CPNP]) и организации (например, [SLA-EXCHANGE]) услуги до ее заверения и исполнения.

Поскольку сложность активации возможностей SDN в значительной мере скрыта от конечных пользователей и обслуживается программами, требуется четкое понимание всей экосистемы для решения вопросов обслуживания этих скрытых сложностей и предотвращения побочного влияния на работу сетей.

Например, системы SDN, предполагающие централизованное принятие решений, должны избегать наличия критических точек отказов. Им недопустимо влиять на производительность пересылки пакетов (например, на транзитные задержки).

Методы SDN не являются обязательными для создания новых сетевых услуг. Базовой сетевой услугой остается (IP) связность, которая запрашивает ресурсы, размещенные в сети. Таким образом, методы SDN можно рассматривать как

[1]Network Management System - система сетевого управления.
[2]Path Computation Element - элемент расчета пути.
[3]Forwarding and Control Element Separation.
[4]Policy Decision Point - точка принятия решения для правил (политики).
[5]Policy Enforcement Point.
[6]Policy Information Base.

другой способ взаимодействия с модулями сетевых служб и вызова ресурсов связности и хранения для выполнения запросов конкретных услуг.

По определению активация и использование методов SDN ограничиваются средствами, поддерживаемыми во встроенных программах и оборудовании. Не следует ожидать, что методы SDN будут поддерживать неограниченный набор настраиваемых функций.

3.3. Сравнение результатов с ожиданиями

Поскольку несколько программных модулей могут управляться внешними объектами (обычно PDP), нужны средства контроля соответствия предоставленного согласованному. Такие средства относятся к методам SDN.

Этим типичным методам, основанным на правилах, следует взаимодействовать как с машинами структурирования услуг (которые предназначены для демонстрации и, возможно, согласования характеристик услуг), так и с сетью для постоянной оценки соответствия поведения сети целям, заданным механизмом структурирования услуг, и целям, которые могут динамически согласовываться с клиентом (например, как указано в CPP [CPP] [CPNP]). Это требование применимо к нескольким участкам сети, включая перечисленные ниже.

1. Интерфейс между двумя смежными провайдерами сетей IP.
2. Интерфейс доступа между сервис-провайдером и провайдером сети IP.
3. Интерфейс между абонентом и провайдером сети IP.

В идеале полностью автоматизированную систему предоставления услуг, включая согласование, заказ, обработку заказа на предоставление, гарантии и исполнение следует поддерживать за счет последствий, рассмотренных в параграфе 4.1. Этот подход также предполагает использование широко распространенных стандартных моделей данных и информации в дополнение к интерфейсам.

3.4. Проектируем осторожно

Предоставление открытых программируемых интерфейсов обеспечивается за счет расширяемости и производительности.

Приветствуется поддержка жестко закодированных методов оптимизации. То же самое относится к интерфейсам, которые позволяют прямое управление некоторыми механизмами (например, маршрутизацией и пересылкой) без каких-либо промежуточных уровней адаптации (например, от базовых объектов к фирменным интерфейсам CLI). Тем не менее, использование фирменного доступа для некоторых механизмов означает, что это может быть выгодно с точки зрения производительности за счет усложнения настройки.

Методы SDN в любом случае должны учитывать фирменные компоненты производителей, поскольку они не перестанут применяться по причине жесткой конкуренции.

Следует избегать или хотя бы тщательно продумывать внедрение новых функций и устройств, которые могут поставить под угрозу гибкость сетей, в свете возможного влияния на производительность и расширяемость. Устройства с поддержкой SDN должны сосуществовать с унаследованными системами.

Развертывание SDN в масштабе сети маловероятно и вместо этого будет последовательно развертываться множество экземпляров разных реализаций SDN, которые будут приспосабливаться к разным сегментам сетей и услуг.

3.5. OpenFlow

Расширение возможностей сетей с управляемыми по основному каналу модулями может опираться на протокол OpenFlow или иные протоколы обмена информацией между уровнями управления и данных.

Действительно, имеется много протоколов, которые можно применить для решения этих и более широких (например, резервирование ресурсов) задач. Пересылка конфигурационной информации, например, может быть реализована на основе таких протоколов как PCEP[1] [RFC5440], NETCONF[2] [RFC6241], COPS-PR[3] [RFC3084], RPSL[4] [RFC2622] и т. п.

Следовательно между OpenFlow и SDN нет однозначной связи. Скорее OpenFlow является одним из возможных протоколов для передачи устройствам конфигурационных данных. Таким образом, OpenFlow является одной из составных частей инструментария SDN.

3.6. Дополнительные соображения

Неизбежные компромиссы между эксплуатацией существующей сетевой экосистемы и внедрением некоторых технологий SDN возможно решаются за счет внедрения новых технологий. Операторам не требуется выбирать, поскольку обе среды должны сосуществовать.

В частности, на развертывание методов SDN могут повлиять приведенные ниже соображения.

- Гибкость полностью программных реализаций ограничивается возможностями программ и оборудования.
- Полностью модульная реализация трудно достижима (по причине неявной сложности) и может потребовать дополнительных усилий для тестирования, проверки и поиска неполадок.
- В полностью централизованной системе управления очевидно будут возникать проблемы расширяемости. Распределенные протоколы и их способность реагировать на некоторые события (например, отказ канала) остаются краеугольным камнем способных к расширению сетей. Это означает, что решения SDN могут опираться на логическое представление централизованных функций (например, уровень абстракции, поддерживающий взаимодействие между PDP).

4. Обсуждение

4.1. Влияние полной автоматизации

Путь к полной автоматизации сталкивается с множеством проблем, включая перечисленные ниже.

- Автоматизация должна быть хорошо реализована для облегчения тестирования (включая проверки пригодности) и поиска неполадок.

[1]Path Computation Element (PCE) Communication Protocol - коммуникационный протокол PCE.
[2]Network Configuration Protocol - протокол настройки сети.
[3]COPS Usage for Policy Provisioning - применение COPS для реализации политики.
[4]Routing Policy Specification Language - язык задания правил маршрутизации.

  - Это требует имитационных инструментов, которые позволят оценить влияние высокого уровня автоматизации на всю процедуру предоставления услуг, чтобы избежать «синдрома безумного робота», последствия которого могут быть значительными в плане контроля QoS и других аспектов.
  - Это также предполагает внимательный учет человеческого опыта, чтобы операторы могли использовать надежные и гибкие средства автоматизации повторяющихся или подверженных ошибкам задач, а затем опираться на автоматизацию или объединение множества операций для решения все более сложных задач с меньшим участием человека (управление и ввод данных).
- Упрощение и ускорение предоставления, гарантий и выполнения услуг, а также обнаружения сетевых отказов, диагностики и анализа причин для оптимизации расходов.
  - Такая оптимизация затрат связана с ускорением предоставления услуг, а также оптимизацией участия людей (см. выше) и глобальными, независимыми от технологий процедурами структурирования и предоставления услуг. В частности, возможность внедрения новых функций в имеющиеся устройства не должна предполагать замены этих устройств, обеспечивая разумную капитализацию вложений.
  - Этого можно достигнуть за счет автоматизации, возможно основанной на логически централизованном представлении сетевой инфраструктуры (или ее части), что ведет к необходимости автоматизации способов обнаружения топологии, устройств и их возможностей, а также рабочих процедур.
  - Основной интеллект сохраняется в PDP, что предполагает фокусировку значительной части усилий, связанных с SDN, на подробной спецификации функций PDP, включая алгоритмы и механизмы состояний и поведения оборудования, основанные на стандартизованных данных и информационных моделях.
  - Эти информационные модели и данные должны быть четко структурированы для обеспечения эффективности и гибкости. Это может предполагать набор упрощенных псевдоблоков, собираемых в соответствии с характером предоставляемых услуг.
- Необходимость уровней абстракции, обеспечивающих четкий интерфейс между субъектами бизнеса и между уровнями. Такие уровни абстракции вызываются в контексте структурирования и представления услуг, упрощая решение перечисленных ниже задач.
  - Представление услуг связности IP для пользователей, партнеров, приложений, поставщиков услуг и содержимого и т. п. (пример можно найти в [CPP]).
  - Решения, согласующие требования связности IP с целями проектирования сетей.
  - Адаптивные процессы динамического принятия решений, которые могут корректно работать в соответствии с входными данными и метриками, такими как текущее использование ресурсов и потребность в них, прогнозы и параметры трафика и т. п. для обеспечения динамического распределения ресурсов и схем исполнения правил.
- Эффективное согласование технологически разнородных сетевых сред за счет указанных ниже мер.
  - Независимые от производителей процедуры настройки, основанные на исполнении не связанных с производителями правил вместо заданных производителями языков.
  - Средства упрощения процедур управления и оркестровки ресурсов.
  - Исключение промежуточных устройств и прямое взаимодействие с системами (например, маршрутизации и пересылки).

4.2. Загрузка SDN

Нужно обеспечить средства динамического обнаружения функциональных возможностей устройств, управляемых PDP, для автоматического предоставления услуг. Это связано с тем, что получение информации о реальных возможностях сети позволит структурировать интеллект PDP для получения информации о правилах предоставления услуг.

Типичным примером является документирование политики организации трафика на основе динамического обнаружения различных функций, поддерживаемых сетевыми устройствами, в зависимости от предоставляемых услуг так, чтобы организация разных маршрутов к одному получателю зависела от типа трафика, местоположения функций, требуемых для пересылки этого трафика, и т. п.

Такое динамическое обнаружение может базироваться на обмене определенной информацией по протоколу IGP или BGP между сетевыми устройствами или между сетевым устройством и PDP в унаследованных сетевых средах. PDP могут также передавать сетевым устройствам незапрошенные команды для получения описаний их функциональных возможностей и определения на основе этих данных топологии сети и сервиса.

Методы SDN (как отмечено в параграфе 2.4) могут быть развернуты в среде без поддержки протоколов IGP и BGP, но процедура начальной загрузки SDN в такой среде предполагает поддержку перечисленных ниже возможностей.

- Динамическое обнаружение участвующих узлов SDN (включая PDP) и их возможностей гибкими средствами, предполагающими взаимную аутентификацию PDP и участвующих узлов (раздел 5). Должна также обеспечиваться защита целостности информации, передаваемой между PDP и участвующими узлами.
- Динамическое подключение PDP к участвующим узлам с предотвращением петель.
- Динамическое включение сетевых услуг в зависимости от возможностей устройства и (возможно) динамического согласования между сервис-провайдером и абонентом.
- Динамическая проверка связности между PDP и участвующими узлами для предоставления данной сетевой услуги (или набора услуг).
- Динамическая оценка области доступности как функции предоставляемой услуги.
- Динамическое обнаружение и диагностика отказов, а также принятие соответствующих мер.

Аналогичным способом следует представлять средства получения описаний (включая базовую конфигурацию) любого сетевого устройства, которое может участвовать в предоставлении данной услуги, чтобы помочь PDP структурировать услуги, которые могут быть предоставлены в зависимости от доступных ресурсов, их расположения и т. п.

Таким образом, в средах без IGP и BGP может потребоваться специальный протокол начальной загрузки для поддержки упомянутых возможностей и корректной работы устройств с поддержкой PDP и SDN в дополнение к возможной потребности в дополнительной сети, которая будет обеспечивать функции обнаружения и связности.

В частности, организация и работа SDN в средах без IGP и BGP должны обеспечивать производительность, аналогичную характеристикам унаследованных сред, где используются протоколы IGP и BGP. Например, базовой сети следует сохранять работоспособность даже при потере соединения с PDP. Кроме того, операторам следует оценить стоимость внедрения нового протокола начальной загрузки по сравнению с интеграцией упомянутых возможностей с имеющимися механизмами протоколов IGP и BGP.

Поскольку связанные с SDN возможности могут встраиваться в имеющуюся сетевую инфраструктуру, не все такие возможности могут быть включены сразу с точки зрения начальной загрузки - может потребоваться поэтапный подход.

Типичным примером развертывания может служить использование процесса принятия решений SDN в качестве платформы эмуляции, которая будет помогать сервис-провайдерам и операторам принимать соответствующие технические решения до их фактического развертывания в сети.

Завершение процедуры обнаружения не обязательно означает полную работоспособность сети. Функциональность сети обычно предполагает надежное решение, основанное на отказоустойчивости и высокой доступности.

4.3. Работа SDN

С точки зрения OAM[1] [RFC6291] при работе сети с поддержкой SDN возникает несколько вопросов, приведенных ниже.

- Как сервис SDN взаимодействует с блоками управления сетью? Например, как результаты динамического согласования параметров услуги с клиентом или группой клиентов в данный период времени будут влиять на процесс принятия решений PDP (распределение ресурсов, расчет пути и т. п.)?
- Что подходит в качестве инструментов OAM для работы в сети SDN (например, для проверки доступности PDP или PEP)?
- Как оптимизировать производительность (например, время предоставления услуги) при управлении программными модулями со стороны внешнего устройства (обычно PDP)?
- До какой степени реализация SDN упрощает управление сетью, включая диагностику сети и служб?
- Следует применять принцип разделения уровней управления и данных к сети или ее части в зависимости от природы предоставляемых услуг или с учетом развернутой в настоящее время технологии?
- Каково влияние на процедуры и методологию тестирования у сервис-провайдеров (проверка пригодности и подготовка к развертыванию)? В частности, (1) как будут определяться и выполняться тестовые сценарии при активации настраиваемых модулей, (2) какова методология оценки поведения управляемых SDN устройств, (3) как выполняется выход из тестового сценария (4) и т. п.
- Как методы SDN влияют на предоставление и гарантии услуг? Как следует оценивать поведение устройств SDN (например, выполнение конфигурационных задач) по сравнению с тем, что было динамически согласовано с клиентом? Как измерять эффективность динамически исполняемых правил в зависимости от предоставляемых услуг? Как оценивать соответствие предоставленного согласованному? Как методы SDN влияют на практику устранения неполадок?
- Возникает ли риск «замораживания» архитектуры в результате возможных проблем при взаимодействии между управляемыми устройствами и контроллером SDN?
- Как внедрение методов SDN влияет на срок службы унаследованных систем? Возникает ли риск (быстрого) устаревания имеющихся технологий по причине их программных или аппаратных ограничений?

Ответы на эти вопросы скорей всего будут разными у каждого сервис-провайдера в зависимости от технологии и требований бизнеса.

4.4. Интеллект остается в PDP

Предложенное в параграфе 2.3 определение SDN предполагает, что интеллект сохраняется на уровне управления или администрирования (или в обоих). Этот интеллект обычно представляется точками принятия решений (PDP) [RFC2753], которые являются одной из важных компонент модели управления на основе правил.

Следовательно, сети SDN опираются на функции PDP, которые способны обрабатывать различные входные данные (прогнозы трафика, результаты согласования между клиентами и сервис-провайдером, состояние ресурсов, показанное в подходящей информационной модели базы PIB и т. п.) для принятия решений.

Устройство и работа такого интеллекта на основе PDP с возможностью расширения остается частью областей, требующих дополнительных исследований.

Очевидно, что для предотвращения излишне централизованных схем нужны связи между PDP, что требует решения связанных с этим вопросов. В домене может быть несколько активных экземпляров PDP. Поскольку каждый из этих экземпляров PDP может отвечать за принятие решений об исполнении конкретных правил (например, PDP для QoS, безопасности и т. п.), требуется схема коммуникаций между PDP для глобальной координации точек PDP.

Может также потребоваться обмен между PDP в разных доменах, примерами которого могут служить (1) обмен информацией при подключении мобильного узла к чужой сети для получения от домашней точки PDP правил для этого узла или (2) взаимодействие PDP для расчета путей между доменами, соответствующих параметрам трафика.

4.5. Простота и адаптивность против сложности

Функциональные метадомены, введенные в параграфе 2.4, предполагают высокий уровень автоматизации от согласования сервиса до его предоставления и работы. Автоматизация важна для простоты, но ее недопустимо считать «волшебной кнопкой», которая позволит администратору одним нажатием решить все задачи по обработке запросов клиента и выделению дополнительных ресурсов.

Удовлетворение потребностей в простоте и адаптируемости за счет автоматизации процедур обычно приводит к усложнению автоматизации.

4.6. Производительность и расширяемость

Сочетание гибкости с программными решениями неизбежно создает проблемы производительности и расширяемости в зависимости от числа и типа предоставляемых услуг и связанной с ними динамики.

[1]Operations and Management - операции и администрирование.

Например, сети ЦОД[1], реализованные на коммутаторах OpenFlow, вряд ли столкнуться с проблемами расширяемости FIB. И напротив, соединения между ЦОД, нацеленные на динамическое управление мобильностью виртуальных машин (VM[2]), возможно на основе определенных правил QoS, могут столкнуться с проблемами расширяемости.

Заявленная гибкость сетей SDN в таком контексте требует тщательного изучения со стороны операторов.

4.7. Оценка рисков

Ниже перечислены возможные риски, которые следует принимать во внимание.

- Зависимость от технологии контроллера вместо зависимости от технологии устройств.
- Возможность «замораживания» системы в результате проблем взаимодействия устройств с контроллером.
- Старение решений SDN в результате программных и аппаратных ограничений. С технической точки зрения возможность динамического предоставления ресурсов в зависимости от предоставляемых услуг может оказаться несовместимой с унаследованными системами маршрутизации, например, в результате их аппаратных ограничений. С экономической точки зрения применение решений SDN для обеспечения гибкости и автоматизации может существенно увеличить капитальные (CAPEX[3]) и операционные (OPEX[4]) расходы.

5. Вопросы безопасности

Безопасность является важным аспектом любой системы SDN, поскольку она обеспечивает надежность и отказоустойчивость взаимодействий между сетью и приложениями для эффективного контроля доступа и оптимизированной защиты ресурсов SDN от атак любого типа. В частности, политике безопасности SDN [SDNSEC] следует обеспечивать надлежащую защиту ресурсов SDN от действий, способных угрожать работе сети или приложений.

Сервис-провайдерам следует определить процедуры оценки надежности программных модулей в узлах SDN. Такие процедуры должны включать оценку поведения программных компонент (под нагрузкой), обнаружение любых уязвимостей, надежное обновление программ и т. п. Эти средства защиты следует активировать при развертывании узлов SDN и применять в процессе работы, что предполагает процедуры обновления программ.

Хотя эти процедуры могут быть не связаны с SDN напрямую (например, оператор умеет обновлять программный код устройств с остановкой обслуживания или без таковой), следует пересмотреть текущую практику с учетом развертывания и эксплуатации SDN.

Взаимодействия между PEP и PDP предполагают необходимость проверить, что (1) PDP имеет право запрашивать у PEP исполнения принятых PDP решений, (2) PEP имеет право передавать запросы PDP (дополнительные данные конфигурации, уведомление по результатам настройки и т. п.), (3) PEP может воспринимать решения PDP и (4) связь между PDP внутри домена или между доменами надежно защищена (например, каждой точке PDP разрешено взаимодействие с партнером и обеспечивается конфиденциальность данных при обмене между PDP).

6. Благодарности

Большое спасибо R. Barnes, S. Bryant, S. Dawkins, A. Farrel, S. Farrell, W. George, J. Halpern, D. King, J. Hadi Salim и T. Tsou за их комментарии. Отдельная благодарность P. Georgatos за плодотворные дискуссии по соединениям SDNI[5].

7. Литература

[AN] Tennenhouse, D. and D. Wetherall, "Towards an Active Network Architecture", Multimedia Computing and Networking (MMCN), January 1996.

[AUTOMATION] Boucadair, M. and C. Jacquenet, "Requirements for Automated (Configuration) Management", Work in Progress, January 2014.

[CPNP] Boucadair, M. and C. Jacquenet, "Connectivity Provisioning Negotiation Protocol (CPNP)", Work in Progress, October 2013.

[CPP] Boucadair, M., Jacquenet, C., and N. Wang, "IP/MPLS Connectivity Provisioning Profile", Work in Progress[6], September 2012.

[LS-DISTRIB] Gredler, H., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and TE Information using BGP", Work in Progress[7], November 2013.

[PN] Campbell, A., De Meer, H., Kounavis, M., Kazuho, M., Vincente, J., and D. Villela, "A Survey of Programmable Networks", ACM SIGCOMM Computer Communication Review, April 1999.

[RFC1383] Huitema, C., "An Experiment in DNS Based IP Routing", RFC 1383, December 1992.

[RFC2622] Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., and M. Terpstra, "Routing Policy Specification Language (RPSL)", RFC 2622, June 1999.

[RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework for Policy-based Admission Control", RFC 2753, January 2000.

[RFC3084] Chan, K., Seligson, J., Durham, D., Gai, S., McCloghrie, K., Herzog, S., Reichmeyer, F., Yavatkar, R., and A. Smith, "COPS Usage for Policy Provisioning (COPS-PR)", RFC 3084, March 2001.

[RFC4655] Farrel, A., Vasseur, J., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, August 2006.

[1]Центр обработки данных.
[2]Virtual Machine.
[3]Capital Expenditure.
[4]Operational Expenditure.
[5]SDN Interconnection.
[6]Работа опубликована в RFC 7297. *Прим. перев.*
[7]Работа опубликована в RFC 7752. *Прим. перев.*

[RFC5440] Vasseur, JP. and JL. Le Roux, "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, March 2009.

[RFC5810] Doria, A., Hadi Salim, J., Haas, R., Khosravi, H., Wang, W., Dong, L., Gopal, R., and J. Halpern, "Forwarding and Control Element Separation (ForCES) Protocol Specification", RFC 5810, March 2010.

[RFC5812] Halpern, J. and J. Hadi Salim, "Forwarding and Control Element Separation (ForCES) Forwarding Element Model", RFC 5812, March 2010.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, June 2011.

[SDNSEC] Hartman, S. and D. Zhang, "Security Requirements in the Software Defined Networking Model", Work in Progress, April 2013.

[SLA-EXCHANGE] Shah, S., Patel, K., Bajaj, S., Tomotaki, L., and M. Boucadair, "Inter-domain SLA Exchange", Work in Progress, November 2013.

Адреса авторов

Mohamed Boucadair
France Telecom
Rennes 35000
France
EMail: mohamed.boucadair@orange.com

Christian Jacquenet
France Telecom
Rennes
France
EMail: christian.jacquenet@orange.com

Перевод на русский язык

Николай Малых
nmalykh@gmail.com