

Способы трансформации сетей к SDN-архитектуре

О. Р. Лапони́на, В.А.Сухомли́н

Аннотация – Рассмотрены способы трансформации основных классов традиционных сетей к SDN-архитектуре, основанной на стандарте OpenFlow, с целью миграции сервисов и приложений традиционных сетевых технологий в OpenFlow-окружение. Описаны возможные сценарии развертывания SDN-сетей, а также типовые сценарии миграции: миграция на уровне конечных точек, миграция всего стека, миграция части стека. Обсуждаются вопросы сетевой безопасности в условиях возрастающего использования SDN, а также вопросы использования инструментальных средств при решении задач миграции.

Ключевые слова – SDN, OpenFlow, плоскость управления, плоскость данных, SDN-устройства, гибридные SDN-устройства, смешанное развертывание SDN, гибридное развертывание SDN.

I. ВВЕДЕНИЕ. КОМПОНЕНТЫ АРХИТЕКТУРЫ SDN

Целью разработки новой сетевой технологии, называемой Software Defined Network (SDN) или Программно-Конфигурируемыми Сетями (ПКПС), является стремление упростить основные сетевые компоненты такие, как маршрутизаторы и коммутаторы, снизить их стоимости и стоимость их обслуживания, а также увеличить пропускную способность сети. Еще одной из важных целей разработки SDN является возможность централизованного управления сетевым трафиком.

Считается, что использование SDN должно значительно улучшить топологическую целостность сети при любых ее изменениях.

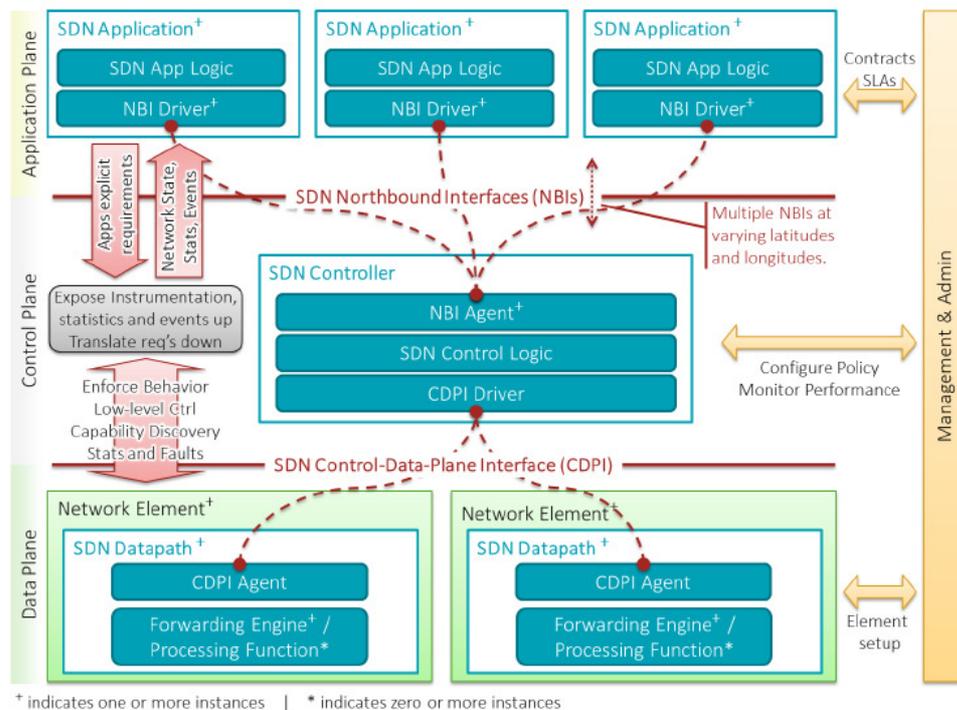


Рис. 1. Общая архитектура SDN

Статья получена 15 марта 2015.

О.Р. Лапони́на – научный сотрудник лаборатории ОИТ, факультета ВМК МГУ имени М.В. Ломоносова (email:laponina@oit.cmc.msu.ru). В.А.Сухомли́н - профессор ВМК МГУ имени М.В.Ломоносова (email:sukhomlin@mail.ru)

Основная идея технологии SDN состоит в том, чтобы:

- Отделить управление сетевым оборудованием от управления передачей данных за счет создания специального

программного обеспечения, которое может работать на обычном компьютере.

- Перейти от управления отдельными экземплярами сетевого оборудования к управлению сетью в целом.
- Создать программно-управляемый интерфейс между сетевым приложением и транспортной средой сети.

Рассмотрим основные компоненты архитектуры SDN. В данной архитектуре различают плоскости (planes) **данных, управления и приложений** (см. рис. 1) [1].

- **SDN-приложение (SDN App)** является программой, которая явно, напрямую, программным способом сообщает SDN-контроллеру свои требования к сети и желаемое поведение сети, используя так называемый NBI-интерфейс. Кроме того, оно имеет возможность получать от SDN-контроллера информацию, обеспечивающую ему целостный взгляд на сеть.

SDN-приложение состоит из единственного компонента, который определяет логику SDN-приложения, и одного или нескольких NBI-драйверов, которые обеспечивают взаимодействие приложения с SDN-контроллером и с другими SDN-приложениями. SDN-приложения могут сами определять более абстрактный уровень управления сетью, создавая один или несколько NBI-интерфейсов более высокого уровня с помощью соответствующих NBI-агентов.

- **SDN-контроллер** является логически централизованной системой, которая
 - Преобразует требования уровня SDN-приложения в команды для устройств выполняющих пересылку данных и поддерживающих технологию SDN, так называемых SDN Datapath.
 - Предоставляет SDN-приложению информацию о сети, в том числе информацию о событиях и различные статистические данные.

SDN-контроллер состоит из одного или нескольких NBI-агентов, управляющей логики и CDPI-драйвера. Определение SDN-контроллера как логически централизованной сущности не обязательно предполагает точную спецификацию таких деталей реализации, как возможное совместное функционирование нескольких контроллеров для защиты от сбоев, возможную иерархию контроллеров, возможную виртуализацию какой-либо части сетевых ресурсов или какую-либо другую взаимную организацию SDN-контроллеров.

- **SDN Datapath** является сетевым устройством, которое обеспечивает перенаправление пакетов и обработку данных, и поведение которого не может быть изменено никакими другими сетевыми устройствами или компонентами, кроме SDN-контроллера.

Логическое описание может охватывать все или только некоторое подмножество физических ресурсов конкретного сетевого устройства.

SDN Datapath состоит из CDPI-агента и набора из одного или нескольких движков (engine) перенаправления трафика, и нуля или более функций обработки трафика. Это устройство может просто выполнять пересылку пакетов между своими внешними интерфейсами, или выполнять требуемую обработку трафика. Один или несколько SDN Datapath могут быть реализованы в единственном физическом сетевом устройстве. Или же единственный SDN Datapath может объединять несколько физических сетевых устройств. Данное логическое определение не предполагает детали реализации, такие как отображение логического представления на физическое, управление разделяемыми физическими ресурсами, виртуализацию или какую-либо другую реализацию SDN Datapath, интероперабельность с не-SDN-сетями или функции обработки данных, включающих функции уровней L4-L7 модели OSI. Взаимодействие между SDN-контроллером и SDN Datapath происходит по протоколу OpenFlow [4], поэтому очень часто такие устройства также называют OpenFlow-устройствами или OpenFlow-коммутаторами.

- **SDN-интерфейс между плоскостями управления и данными (CDPI)** является интерфейсом, определенным между SDN-контроллером и SDN Datapath. Данный интерфейс должен обеспечивать как минимум следующие возможности:

- Программное управление всеми операциями перенаправления.
- Получение всевозможных статистических отчетов от OpenFlow-коммутаторов.
- Оповещения о событиях.

Предполагается, что CDPI будет реализован открытым, не зависимым от производителя и интероперабельным способом. Протоколом, который обеспечивает взаимодействие плоскости управления и плоскости данных, является протокол OpenFlow.

- **SDN Northbound интерфейсы (NBI)** являются интерфейсами между SDN-приложениями и SDN-контроллерами. Они предоставляют абстрактный взгляд на сеть и непосредственно обеспечивают необходимое сетевое поведение. Они могут быть реализованы на любом уровне абстракции и с различным набором функциональностей.

Плоскость данных состоит из элементов сети, чьи SDN Datapath (OpenFlow-коммутаторы) имеют параметры, которые устанавливаются агентом интерфейса плоскости управления данными (CDPI). SDN-приложения выполняются в плоскости приложений и взаимодействуют друг с другом посредством драйверов NorthBound

интерфейса (NBI). На среднем уровне SDN-контроллер преобразует информацию от NBI в плоскость данных Datapath и предоставляет соответствующую информацию SDN-приложениям. Плоскость управления и администрирования (Management & Admin) отвечает за конфигурирование сетевых элементов уровней SDN Datapath и SDN-контроллера, а также конфигурирует политики, определяющие область управления данного SDN-контроллера или SDN-приложения. Данная архитектура SDN-сети может сосуществовать с не-SDN-сетью, особенно на этапе трансформации традиционной сети к SDN-сети.

Предполагается, что NBI будет реализован открытым, не зависимым от производителя и интероперабельным способом.

- **Драйверы и агенты интерфейса.** Каждый интерфейс реализуется парой драйвер-агент, агент является «южной», или нижней стороной, повернутой к инфраструктуре, драйвер является «северной», или верхней стороной, повернутой к приложению.
- **Администрирование** охватывает статические задачи, которыми лучше управлять извне плоскостей приложения, управления или данных. Примерами являются управление взаимодействием между провайдером и клиентом, выделение ресурсов клиентам, параметры установки физического оборудования, координация доступности и управление credenциалами логических и физических сущностей. Взаимодействие сущностей администрирования находится вне предметной области архитектуры SDN. Одной из целей SDN является решение на уровне SDN многих задач управления, которые решаются на уровне передачи данных в традиционной сети.

В архитектуре SDN **приложение может знать о сети всё**, в противоположность традиционным сетям, в которых сеть знала всё о приложении. А именно:

- Традиционные приложения (т.е. не-SDN) только неявно и косвенно описывают свои требования к сети, обычно включающие несколько шагов, которые выполняет сам человек. Например, ведутся переговоры о необходимых ресурсах и об управлении политикой поддержки приложения.
- Традиционные сети (т.е. не-SDN) не имеют способа динамически указать полный диапазон требований пользователя, например, пропускную способность, диапазон допустимых задержек или другие характеристики доступности. Заголовки пакетов могут содержать запросы приоритета, но сетевые провайдеры обычно не доверяют пользовательской маркировке трафика. В результате некоторые сети сами

пытаются сделать заключение о пользовательских требованиях (например, посредством анализа трафика), что может внести дополнительную стоимость управления и привести к неправильному определению пользовательских требований. Технология SDN позволяет пользователю полностью указать свои требования к сети, которые могут быть затем монетизированы.

- Традиционные сети не раскрывают информацию и состояние сети приложениям, использующим их. Используя технологию SDN, SDN-приложения могут следить за состоянием сети и адаптироваться соответствующим образом.

Плоскость управления

- (1) Логически централизована.
- (2) Отделена от плоскости данных.

SDN-контроллер информирует о состоянии сети приложения и преобразует требования приложений в низкоуровневые правила для OpenFlow-коммутаторов. Тем не менее, это не означает, что контроллер физически централизован. Для обеспечения производительности, масштабируемости и/или надежности логически централизованный контроллер может быть распределен таким образом, чтобы несколько экземпляров физических контроллеров кооперировались для управления сетью и обслуживания приложений.

Решения по управлению принимаются на основе текущего глобального взгляда на состояние сети, а не на основе распределенного изолированного поведения каждого сетевого шага (hop). В SDN плоскость управления функционирует как единая, логически централизованная сетевая ОС, используя термины планирования и разрешения конфликтов ресурсов, абстрагируясь от аппаратных деталей низкого уровня.

SDN-контроллер полностью управляет SDN Datapath, что упрощает планирование и распределение ресурсов.

II. КАТЕГОРИИ СЕТЕЙ

В рассматриваемом случае все сети разделим на следующие категории, не претендуя на полноту классификации: глобальные сети или WANs (Wide Area Networks), к которым подключены сети интернет-сервис-провайдеров (ISP - Internet service providers), сети центров обработки данных (ЦОДов), сети предприятий и сети кампусов.

Рассмотрим основные характеристики каждого класса сетей и наметим подходы трансформации каждого класса сетей к сетям с SDN-архитектурой.

- **Сети кампусов или CANs (Campus Area Networks)** - компьютерные сети, соединяющие локальные сети на

географически ограниченном пространстве, например, университетского городка, зданий корпорации или военной базы. Компоненты сети кампуса обычно соединены магистральной сетью, которая соединена с одним или несколькими ЦОД через WAN. Как правило, сеть университетского кампуса включает логические сети и части ЦОД, принадлежащие различным департаментам или институтам, а также ИТ-ресурсы учебного заведения.

- **ЦОД предприятий** могут отличаться по размеру, но обычно состоят из сетевых ресурсов, используемых для подсоединения различных подсетей к серверам (физическим или виртуальным), а также к хранилищам данных. Для этих сетей должна обеспечиваться высокая степень информационной безопасности и защиты, а также предоставление специальных сетевых функций, как, например, балансировка нагрузки. Требования к сетевому ПО могут различаться, но приложения, выполняющие эти сервисы, должны иметь достаточно высокий приоритет.
- **ЦОД, предоставляющие услуги по аренде**, получают значительные преимущества от внедрения SDN. Эти ЦОД имеют много общего с ЦОДами предприятий, при этом арендаторы обычно разделяют общие физические ресурсы. В сетях таких ЦОД виртуализация вычислительных ресурсов является необходимостью, при этом необходимо обеспечение таких сервисов, как балансировка нагрузки, поддержка непрерывности обслуживания и восстановление при сбоях. В таких сетях важным компонентом архитектуры являются программируемые сетевые устройства или программные коммутаторы, обеспечивающие как гибкость, так и производительность ЦОДов.
- **WAN-сети и сети сервис-провайдеров** характеризуются тем, что требования к этим сетям могут сильно различаться. Однако тенденция перехода для сетей ISP к технологии SDN очевидна. Так, например, такой ISP, как Google, использует именно технологию SDN и OpenFlow-коммутаторы для управления своими внутренними ресурсами.

III. ТРЕБОВАНИЯ К СПОСОБУ МИГРАЦИИ

Согласно разработанной ISO [2] концепции сетей будущего (Future Networks), переход к новым сетевым технологиям может занять значительный временной интервал. Поэтому центральной идеей в построении сетевой инфраструктуры становится сетевая **федерация**, в

реализации которой важную роль играют методы сетевой виртуализации. Именно консолидация на этой основе сетевых технологий с различной архитектурой и интероперабельность сетевых компонентов обеспечивает необходимые условия для миграции (переноса) сервисов и приложений между сетевыми технологиями. При этом миграция подразумевается в обе стороны - как со стороны унаследованных решений на новые сетевые технологии, так и со стороны новых сетевых технологий на унаследованные или специализированные решения. В данной работе нас будет интересовать только переход от текущих сетевых технологий к новым, а именно, трансформация первых к SDN-сетям. Конечной целью такого перехода и является миграция используемых сервисов и приложений в новые сетевые окружения. Поэтому в дальнейшем под термином миграция будет пониматься весь переход от старых сетевых решений к новым. Заметим, что выбор способа миграции определяется основными требованиями к целевой сети, требованиями к самому процессу миграции исходной сети, возможными этапами миграции и, наконец, требованиями тестирования для гарантии полноты и успешности миграции сети.

Процесс миграции на сеть, основанную на SDN, может быть связан со значительными рисками. Простой при миграции, обесценивание инструментальных средств диагностики и мониторинга или сложность и производительность новой технологии – все эти возможные риски должны быть предварительно рассмотрены и проанализированы.

Будем предполагать, что при миграции с традиционной сети на сеть с использованием SDN должны быть выполнены следующие требования.

- а) Целевая сеть должна поддерживать гетерогенность, обеспечивая совместное использование многочисленных устройств от различных производителей. Миграция сервисов должна рассматриваться именно в такой гетерогенной инфраструктуре. Должны быть определены способы миграции, специфичные для каждого типа сетевого компонента, а также должна быть определена сетевая инфраструктура и инструментальные средства общей оркестровки.
- б) Целевая сеть должна быть ориентирована на выполнение сервисов, для которых обеспечивается отказоустойчивость и автоматическое выполнение обновлений ПО.
- в) Целевая сеть должна поддерживать необходимое ПО, инструментальные средства (ИС) и симуляторы. Существующие ИС должны быть протестированы на возможность работы с целевой сетью, либо необходимо обеспечить их прозрачное функционирование.

г) Должны быть определены этапы миграции. Для исходной сети может потребоваться трансформация ее в некоторое промежуточное состояние, из которого и будет осуществляться дальнейшая миграция.

IV. ТИПЫ СЕТЕВЫХ УСТРОЙСТВ

Сетевые устройства можно разделить на наследуемые, OpenFlow-устройства и гибридные.

Наследуемыми устройствами являются традиционные коммутаторы и маршрутизаторы со встроенными возможностями управления и перенаправления.

OpenFlow-устройствами являются коммутаторами с поддержкой только уровня перенаправления; уровень управления расположен во внешнем компоненте, взаимодействие с которым осуществляется по протоколу OpenFlow. Гибридные OpenFlow-коммутаторы могут, как сами обеспечивать управление сетевым трафиком, так и предоставлять возможности OpenFlow.

V. ОСНОВНЫЕ СПОСОБЫ РАЗВЕРТЫВАНИЯ SDN

Трансформация исходной сети к SDN с миграцией на целевую сеть сервисов и приложений реализуется поэтапно [3]. На протяжении этого процесса в сеть будут вводиться OpenFlow-устройства, которые будут работать с существующими устройствами, при этом сетевые операции будут осуществляться как имеющимися устройствами управления, так и контроллерами и конфигураторами OpenFlow (Рис.2). После того, как сервисы исходной сети мигрируются на целевую SDN-сеть, исходная система управления сетью, включая устройства управления и наследуемые коммутаторы и маршрутизаторы, удаляется.

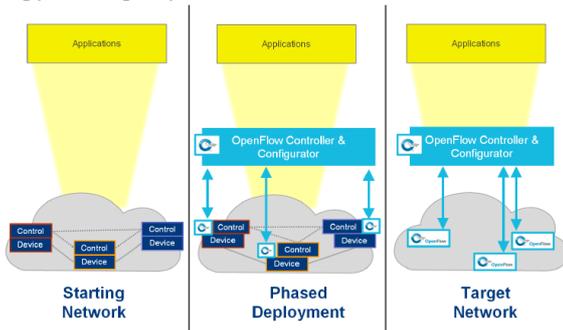


Рис. 2. Миграция в несколько этапов

Процедура миграции может быть частичной, когда, например, на границах домена поддерживается SDN, а весь домен не поддерживает. Это может также включать случаи, когда только отдельные домены поддерживают SDN, а некоторые соседние домены не поддерживают (Рис.3).

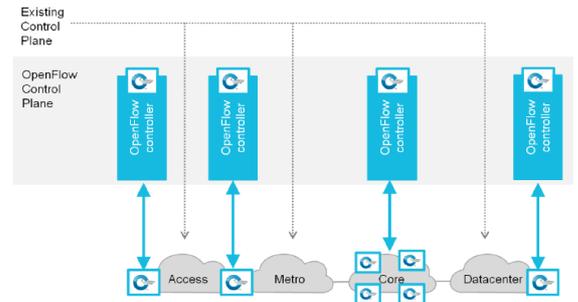


Рис. 3. Возможные сетевые развертывания

Для реализации процедуры миграции можно предложить следующие способы:

- **Развертывание «с чистого листа»:** в этом случае никакого другого сетевого оборудования не существует, и нет необходимости поддерживать наследуемое оборудование (Рис.4).

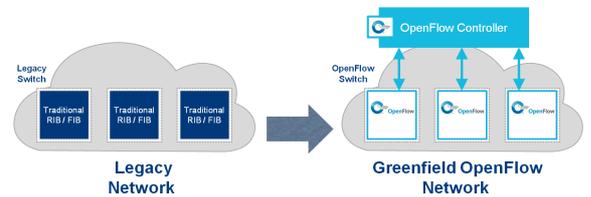


Рис. 4. Способ развертывание «с чистого листа»

- **Смешанное развертывание:** данный способ миграции предполагает, что новые OpenFlow-устройства развертываются и сосуществуют совместно с традиционными коммутаторами и маршрутизаторами и должны взаимодействовать с наследуемыми способами управления (Рис.5). Новый OpenFlow-контроллер и традиционные устройства должны обмениваться друг с другом маршрутной информацией.

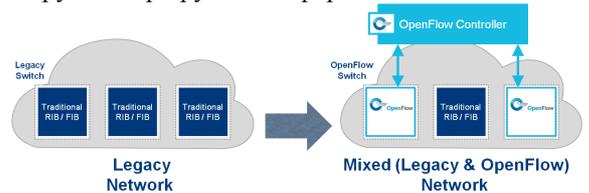


Рис. 5. Смешанное развертывание

- **Гибридное развертывание:** в этом случае должны сосуществовать как устройства, участвующие в смешанном развертывании, так и гибридные устройства с наследуемой и OpenFlow функциональностями. В этом случае гибридные устройства взаимодействуют как с OpenFlow-контроллером, так и с наследуемым способом управления (Рис.6).

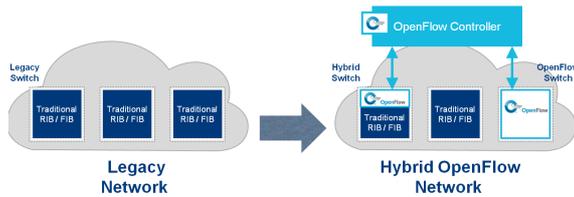


Рис. 6. Гибридное развертывание

Смешанный и гибридный способы миграции являются примерами миграционных подходов, выполняемых в несколько этапов. В любом случае при таких подходах предполагается, что миграция осуществляется в одном сетевом домене.

VI. СЕТЕВЫЕ УРОВНИ, ЗАТРАГИВАЕМЫЕ ПРИ МИГРАЦИИ

Выбор способа миграции на SDN зависит не только от того, какому из рассмотренных классов сетей принадлежит исходная сеть. Многообразие способов миграции обусловлено и тем, что процесс миграции может затрагивать несколько уровней модели сетевого взаимодействия OSI. Хотя первоначально архитектура и функциональные возможности SDN в основном выполнялись на уровне 2 (L2), технология SDN и протокол OpenFlow непрерывно развивались, и в настоящее время стали охватывать все сетевые уровни/поуровни, включая уровень L0 [4]. В текущей практике реализации сетевого взаимодействия различные уровни плана данных связаны с различными уровнями планов управления и приложений, и, следовательно, требуют собственных способов миграции; примерами являются приложения, которым необходимо изменять что-либо на более низких уровнях, или сервис, основанный на глубоком анализе пакета.

По нашему определению гибридное устройство является устройством, которым может управлять как OpenFlow-контроллер, так и наследуемая система управления. В реальных сетях отдельное устройство может функционировать на нескольких уровнях. В результате, могут использоваться несколько систем управления, а также несколько OpenFlow-контроллеров. На Рис.7 показан пример таких сложных сетей, в которых могут мигрировать отдельные сетевые уровни или сразу несколько сетевых уровней.

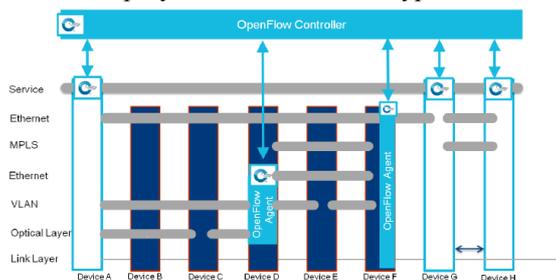


Рис. 7. Влияния миграции на определенные сетевые уровни

На рисунке показано, как отдельные физические устройства обеспечивают доставку пакетов между конечными точками сети. В показанном примере устройство **A** обеспечивает связность на уровне L0, добавляя содержимое VLAN (virtual local area networks)/Ethernet в данные физического уровня. Будем предполагать, что данное устройство может иметь возможности OpenFlow-перенаправления для принятия решения о том, какой физический канал использовать.

Устройство **B** является просто коммутатором физического уровня, на котором сигнал (содержимое) не терминируется. Устройство **C** является коммутатором, который просто добавляет VLAN-заголовки, возможно, выполняя «кросс-соединение» в другую VLAN.

Устройство **D** может являться широкополосным сетевым шлюзом. Такие устройства могут функционировать в широком диапазоне сетевых уровней. Так как данная позиция является важной в сети, в данной точке часто создаются сетевые сервисы. На рисунке не показано, что здесь выполняется терминация уровня L3, но показано, что Ethernet-фрейм передается с использованием различных технологий и управляющих машин. Также показан тот факт, что OpenFlow может функционировать на нескольких уровнях внутри устройства **D**, и, как следствие, несколько OpenFlow-контроллеров могут управлять этим устройством.

Устройство **E** является промежуточным Ethernet-коммутатором или MPLS-устройством, которое не терминирует помеченный коммутируемый путь (LSP). Устройства **F** и **G** являются MPLS-коммутаторами, которые либо перенаправляют, либо терминируют LSP.

Наконец, устройство **H** является Ethernet-устройством, которое видит только Ethernet-кадры, поступающие на его порт, и определяет, как и куда далее доставлять Ethernet- кадр.

VII. ВОЗМОЖНЫЕ СЦЕНАРИИ МИГРАЦИИ

Определим, как проблемы «реального мира» могут влиять на подходы к миграции сети. Рассмотрим три возможных сценария миграции, выделяя устройства или уровни, которые затрагивает изменение.

- **Миграция А – миграция на уровне конечных точек** (Рис.8) означает миграцию «с чистого листа», когда все устройства функционируют на одном и том же уровне (уровнях). Все устройства, участвующие в миграции, являются устройствами, полностью поддерживающими OpenFlow, и управляемыми единственным OpenFlow-контроллером.

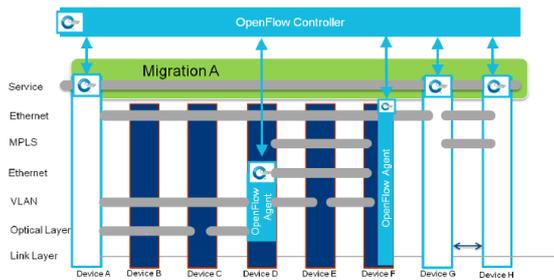


Рис. 8. Пример миграции между конечными точками

- **Миграция В – миграция всего стека:** в данном примере (Рис.9) устройство **F** является гибридным устройством, устройство **G** является полностью OpenFlow-устройством. Устройство **F** всё ещё может находиться под управлением наследуемой системы управления, но в то же самое время может выполнять команды OpenFlow-контроллера. Это пример гибридной миграции сети.

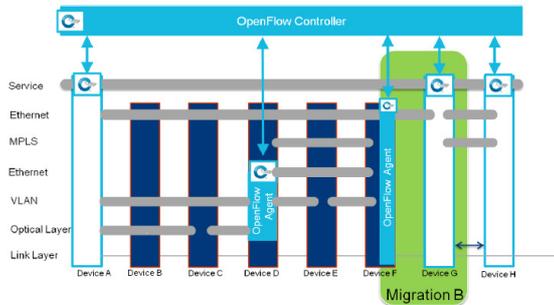


Рис. 9. Пример миграции всего стека

- **Миграция С – миграция части стека** (Рис.10): только некоторая часть уровней устройства мигрирует на OpenFlow (как правило, это уровни Ethernet, VLAN и физический), при этом уровни выше и ниже (MPLS и Ethernet) могут продолжать использовать существующие управляющие системы и протоколы, но выбранные уровни заменяются на OpenFlow. Например, в данной точке сети OpenFlow и OpenFlow-контроллеры могут использоваться для управления возможностями оптики, многопротокольной коммутация по меткам MPLS, цепочки сервисов.

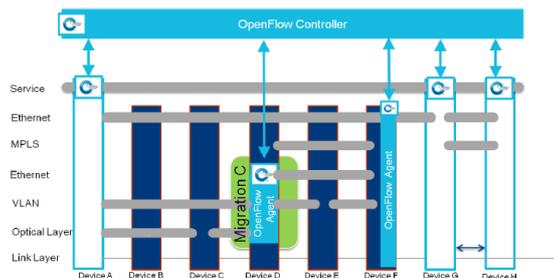


Рис. 10. Пример миграции части стека

Развертывание SDN, основанной на OpenFlow, предполагает наличие одного или нескольких устройств, имеющих поддерживающих протокол OpenFlow агентов, и управляемых логически централизованным OpenFlow-контроллером. Физически контроллер и агент могут быть централизованными и установленными на сервере или быть встроенными в несколько или во все OpenFlow-устройства перенаправления.

Особенности OpenFlow-трафика между контроллером и агентом могут наложить определенные требования к производительности. Данный трафик может возникать как редко, так и достаточно часто, например, для поддержки миграции виртуальных машин (VM) внутри ЦОД. Трафик между контроллером и агентом может состоять из протоколов, которые не мигрированы на OpenFlow, таких как DHCP, PAP, CHAP и более поздних протоколов IPTV и 3GPP. Такой трафик может быть как продолжительным, так и носить взрывной характер. Наконец, любые возникающие исключительные потоки к контроллеру должны быть полностью специфицированы. Также должен специально рассматриваться случай, когда весь трафик должен перенаправляться контроллеру.

Далее должны быть рассмотрены возможные типы потоков, передаваемых по SDN. Например, если трафик является исключительно голосовыми данными в реальном времени, то требования в этом случае должны существенно отличаться от требований, когда трафик представляет собой многопоточное видео. Другими словами, должно быть четкое описание шаблонов трафика.

VIII. ОБСУЖДЕНИЕ БЕЗОПАСНОСТИ

Безопасность сетей является важным фактором, особенно в условиях возрастающей миграции в облака и возрастающего использования SDN. SDN характеризуется централизованной моделью управления, которая обладает достаточной гибкостью для предотвращения сетевых угроз. В современных сетях необходимы не патентованные и более узконаправленные решения, связанные с безопасностью. SDN может быть использован для изменения пути прохождения трафика, основываясь на анализе трафика и статистических данных, предоставляемых контроллером.

В процессе миграции, включая тот период, когда наследуемые сети и SDN-сети будут сосуществовать совместно, требуется поддержка безопасности и изоляция сетей. Необходимо, чтобы существующие сервисы безопасности могли быть мигрированы на SDN-сети.

Один из способов миграции сервисов безопасности на SDN-сеть состоит в следующем:

1. Добавить экспериментальный сетевой слой (например, VLAN).

2. Протестировать этот экспериментальный слой с помощью открытых решений по безопасности SDN.
3. Включить решения по безопасности OpenFlow и SDN в этот новый сетевой слой (VLAN).
4. Начать использовать этот новый сетевой слой.

IX. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА И МЕТРИКИ

Выше были рассмотрены различные подходы к миграции на SDN-сети. На разных этапах миграции могут использоваться различные инструментальные средства, обеспечивающие мониторинг, конфигурирование, управление, тестирование и проверку работоспособности всей сети на протяжении всех этапов миграции [5, 6]. Мониторинг включает сбор метрик в исходной и целевой сетях. Целью сбора метрик является оценка производительности сети и сервисов. Во многих случаях метрики исходной сети могут применяться и при тестировании целевой сети.

Рассмотрим общие характеристики инструментальных средств и метрик, которые могут быть использованы на различных этапах миграции на SDN, включая анализ исходной сети, этапы миграции. Эти метрики должны обсуждаться в терминах «следует иметь» или «желательно иметь» и могут анализировать различные параметры сети, включая функциональные, производительность и т.п.

Существуют сотни не относящихся к SDN метрик, которые могут использоваться для традиционных сетей. Многие из них могут использоваться на стадии миграции на SDN. Однако для SDN-сетей должны быть разработаны новые метрики, относящиеся к сообщениям протокола OpenFlow, OpenFlow-контроллерам и OpenFlow-коммутаторам.

Основные свойства метрик и инструментальных средств.

Существует несколько функциональных характеристик инструментальных средств, с использованием которых можно определить успешность миграции с традиционной сети на OpenFlow-сеть. Эти инструментальные средства должны анализировать проблемы, связанные с безопасностью, масштабируемостью, избыточностью, а также анализировать функциональные возможности, связанные с потоками данных, форматами ввода/вывода, аутентификацией пользователей. Метрики должны собирать информацию и тестировать следующие функциональные характеристики SDN-сети:

1. Оркестровка и управление.
 - Интероперабельность.
 - Резервирование и надежность.
2. Масштабируемость.

3. Смешанные/гибридные развертывания. Любые инструментальные средства, используемые на этапе миграции, должны поддерживать гетерогенные сетевые окружения, содержащие элементы различных производителей, а также компоненты и устройства, добавляемые в целевую сеть.
4. Стратегии отката. Наличие стратегии отката и создания контрольных точек является фундаментальным требованием для больших сетей. Это позволяет отслеживать любые сделанные изменения с помощью GUI или CLI инструментального средства миграции. Инструментальные средства миграции должны иметь возможность выполнять backup, делать моментальный снимок текущего состояния и конфигурации и выполнять откат к предыдущему состоянию.
5. Аутентификация.
6. Открытая среда разработки (framework). API определяет, как внешние инструментальные средства должны взаимодействовать с ПО и позволяет им быть полностью интегрированным в существующее окружение. Инструментальные средства миграции должны предоставлять открытый API для взаимодействия с контроллером и другими приложениями, развернутыми в сети.
7. RBAC. Механизм RBAC определяет доступ к системам на основе аутентификации и ролей пользователя. Инструментальные средства миграции должны обеспечивать доступ на основе ролей к контроллеру и другим OpenFlow-устройствам.
8. Сетевая симуляция. При любом сетевом развертывании возможность симулировать сети для выполнения тестирования возможностей различных сетевых элементов и поведения всей сети является существенным фактором.

X. ЗАКЛЮЧЕНИЕ

В статье рассмотрены способы трансформации основных классов традиционных сетей к SDN-архитектуре, основанной на стандарте OpenFlow, с целью миграции сервисов и приложений традиционных сетевых технологий в OpenFlow-окружение. Описаны возможные сценарии развертывания SDN-сетей: развертывание «с чистого листа», смешанное развертывание, гибридное развертывание. Также описаны типовые сценарии миграции: миграция на уровне конечных точек, миграция всего стека, миграция части стека. Обсуждаются вопросы сетевой безопасности в условиях возрастающего использования SDN, а также вопросы использования инструментальных средств при решении задач миграции.

БИБЛИОГРАФИЯ

- [1] Open Networking Foundation «SDN Architecture Overview», 2013, 5p.
- [2] ISO/IEC DTR 29181-1. Future Network: Problem Statement and Requirements – Part 1: Overall Aspects
- [3] Open Networking Foundation «Migration Use Cases and Methods», 2013, 61p.
- [4] Proceedings of the 16th International Telecommunications. Network Strategy and Planning Symposium (Networks 2014), September 2014, Funchal, Madeira Island, Portugal. Slavisa Aleksic, Igor Miladinovic/ Network Virtualization: Paving the Way to Carrier Clouds. 279p. (<http://toc.proceedings.com/24179webtoc.pdf>)
- [5] Open Networking Foundation «Migration Tools and Metrics», 2014, 23p.
- [6] Open Networking Foundation «OpenFlow Switch Specification», 2012, 205p.

Methods for transforming networks to the SDN-architecture

Olga Laponina, Vladimir Sukhomlin

Abstract - The article describes the main classes of methods for transforming legacy networks to SDN-architecture based on OpenFlow-standards for the purpose of migration services and applications of traditional network technologies in OpenFlow-environment. It describes the possible deployment scenarios of SDN-networks: the deployment of "from scratch", a mixed deployment, hybrid deployment. Also described are typical scenarios of migration: End-to-End Migration, Migration with Full-Stack Handoff, Partial Stack Migration. The issues of network security in the conditions of the increasing use of SDN are discussed, as well as the use of tools for solving problems of migration.

Keywords - SDN; OpenFlow; SDN-devices; hybrid SDN-unit; mixed deployment of SDN; hybrid deployment of SDN; services and applications migration; network security.