

## Методы миграции от сетей традиционной архитектуры к программным-конфигурируемым сетям на основе OpenFlow

# 06, июнь 2014

Маннанов А. Д., Сурков Л. В.

УДК: 004.72

Россия, МГТУ им. Баумана

[mr.mannanov@gmail.com](mailto:mr.mannanov@gmail.com)

[srk@bmstu.ru](mailto:srk@bmstu.ru)

### Введение.

Данная секция описывает подходы и структуру миграции, а также рассмотрены основные положения для рабочей группы по переходу к ПКС. Следующие пункты должны быть отражены рабочей группой в документации:

- 1) Поведение сети с разработанными инструкциями и рекомендациями.
- 2) Требования к целевой сети и к ядру сети. Требования будут различаться между исходной традиционной сети и программно-конфигурируемой сети.
- 3) Определение целей по упрощению сети, а также по снижению затрат на производительность выполнения одной операции, что способствуют к уменьшению загрузки сети.
- 4) Сама миграция является источником риска. Перебои, нарушения в работе сети (по информации от систем мониторинга и диагностики), или рост загрузки – каждый пункт должны быть отражен в документах и инструкциях.

Основываясь на стандарте OpenFlow, следующие требования к программному обеспечению должны быть отражены:

- 1) Целевая сеть должна иметь возможность дополнения функционала благодаря Application Programming Interfaces (API).
- 2) Целевая сеть должна поддерживать динамические обновления программного обеспечения с минимальными прерываниями работы, а также автоматический возврат в случае неверной установки (rollback).
- 3) Целевая сеть должна быть мультивендорной, т.е. с поддержкой устройств от различных производителей. Сервисная поддержка при миграции должна принять инфраструктуру как мультивендорную.
- 4) Целевая сеть должна быть реализована инструментами, программным обеспечением и симуляторами. Или существующие инструменты должны демон-

- стрировать работу целевой сети, или альтернативные инструменты, или должна быть полная ясность в операционной работе.
- 5) Исходной сети может потребоваться подготовка, и необходимо ее трансформировать в промежуточное состояние, из которого миграция сети будет проходить безопасно.
  - 6) После завершения миграции целевая сеть должна соответствовать требованиям и ожиданиям, описанных заранее инструкциями и документациями.

### 1.1 Подходы миграции.

Существует два подхода по осуществлению миграции. Первый подход изображен на рисунке 1. Это прямой метод обновления существующего сетевого оборудования с OpenFlow Agents (оборудование, которое поддерживает программное обеспечение OpenFlow) и вывод управление в OpenFlow контроллер и конфигуратор.

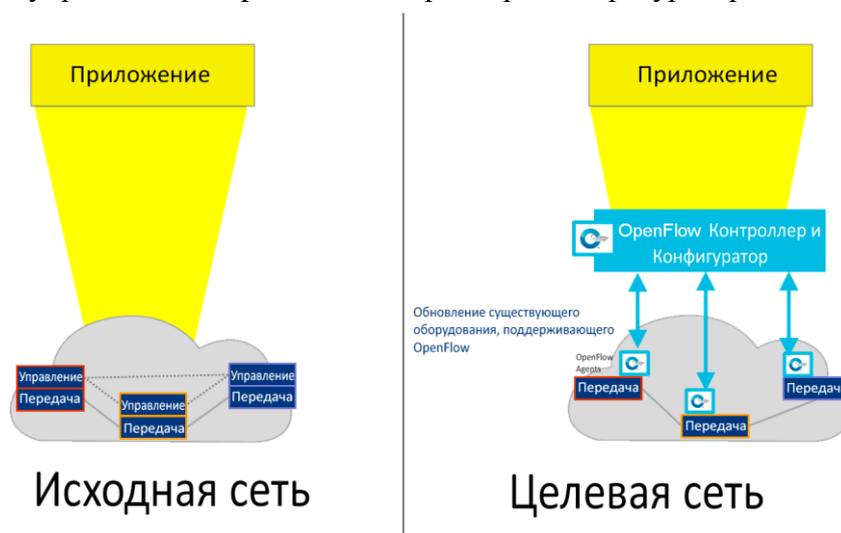


Рисунок 1 – Прямое обновление.

Второй подход выполняется поэтапно. Подход изображен на рис. 2, в котором OpenFlow устройства разворачиваются совместно с существующими сетевыми устройствами. Сетевые операции поддерживаются и выполняются текущим устройством на уровне управления или OpenFlow контроллером и конфигуратором.

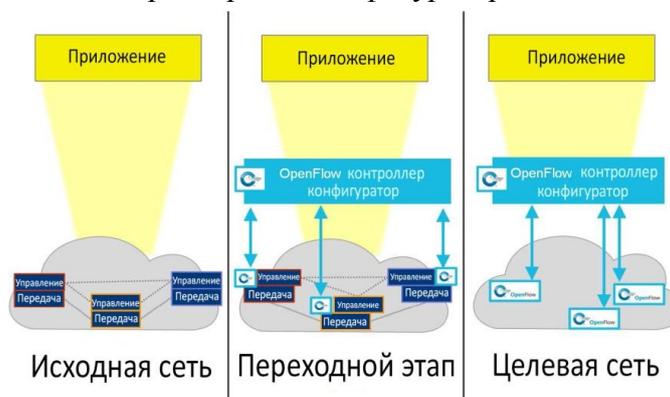
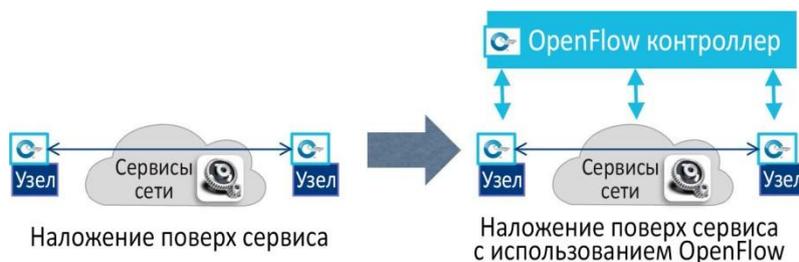


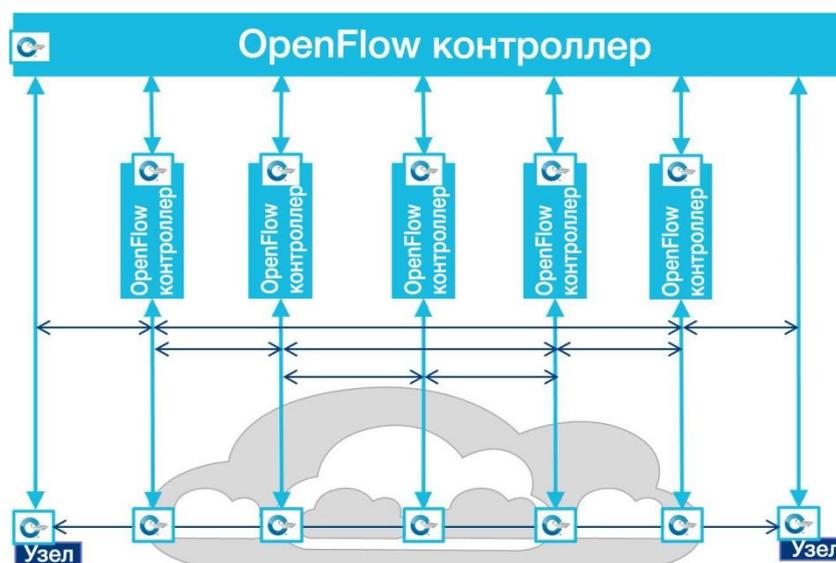
Рисунок 2 – Поэтапная миграция.

В зависимости от реализации сети, процесс миграции и подходы могут быть различными. Например, миграция может включать как прямой метод обновления устройств с OpenFlow агентами, так и поэтапный метод – параллельное внедрение OpenFlow устройств в существующую сеть. Также возможно использование специальных площадок для тестирования и разработок ПКС технологий.

Дополнительно процесс миграции включает в себя включение контроллеров поверх сети (рис. 3) и иерархичное управление OpenFlow (рис. 4).



**Рисунок 3** – Внедрение устройств поверх сети



**Рисунок 4** – Иерархичное управление

Также существуют частичный метод миграции в пределах сетевых устройств, где OpenFlow поддерживается (между уровнем доступа и метро уровнем на рис. 5). Или внедрение ПКС в пределах сети, где есть поддержка OpenFlow, но в соседних зонах ее нет (рис. 5).

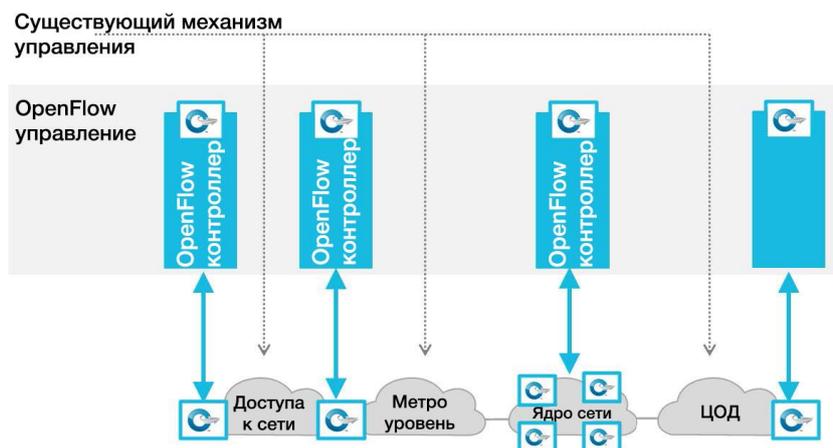


Рисунок 5 – Метод частичной миграции, где соседние устройства не поддерживают OpenFlow.

## 1.2 Методы миграции - детальное рассмотрение.

Все сетевые устройства разделяются на 3 категории с точки зрения OpenFlow решений: 1) традиционная архитектура; 2) OpenFlow архитектура; 3) гибридная архитектура.



Рисунок 6 – Категории сетевых устройств.

Сетевые устройства с традиционной архитектурой включают в себя уровень управления и уровень передачи. Устройства OpenFlow включают в себя только уровень передачи, уровень управления вынесен в отдельное устройство. Гибридные устройства способны работать как с OpenFlow устройствами, так и с сетевыми устройствами традиционной архитектуры.

Рассмотрим подходы миграции в соответствии категорий сетевых устройств. И формализуем определения:

- 1) «Чистая» установка – это метод миграции, при котором все сетевые устройства подвергаются либо полной замене, либо обновлениям. Управляющие устройства заменяются на OpenFlow контроллер.

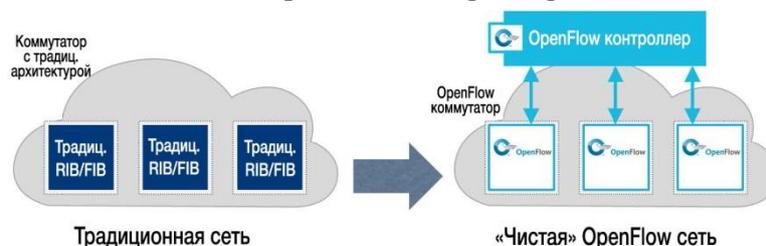


Рисунок 7 – «Чистая» установка.

- 2) Смешанная установка – это метод миграции, при котором внедренные OpenFlow устройства будут взаимодействовать с существующими в сети устройствами традиционной архитектуры. Внедренный OpenFlow контроллер и устройства традиционной архитектуры должны обмениваться маршрутной информацией друг с другом через устройство управления.

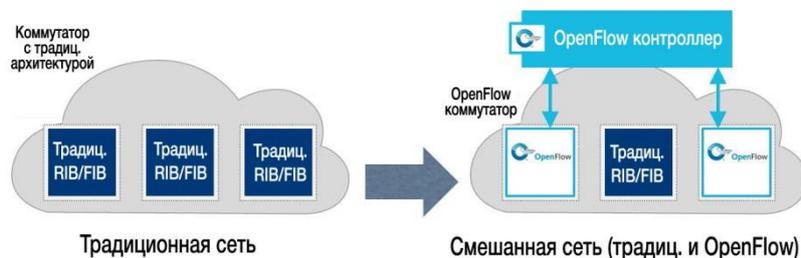


Рисунок 8 – Смешанная установка.

- 3) Гибридная установка – это метод внедрения ПКС, при котором в смешанную сеть внедряются гибридные устройства, поддерживающие OpenFlow функциональность.



Рисунок 9 – Гибридная установка.

Смешанные и гибридные миграции являются примерами поэтапной миграции. Все эти примеры предполагают один домен сети во время миграции. В большинстве случаев переход к OpenFlow обусловлен наличием дополнительных возможностей. Другими словами, использование OpenFlow желательно из-за наличия end-to-end услуг. На рисунке 3 изображена возможность использования этих услуг поверх сети. Чтобы использовать возможности таких услуг, необходимо внедрение OpenFlow контроллера с устройствами, поддерживающими OpenFlow, в любой из конфигураций: «чистая», смешанная или гибридная.

Когда рассматривается сеть, то в большинстве случаев сеть не состоит из одного домена. На самом деле сеть может состоять из множества разнородных уровней сетевой модели, каждая из которых должна быть связана с OpenFlow. Например, когда внешние устройства связаны Ethernet потоками с другими конечными устройствами на VLAN. Внутренние устройства представляют собой два MPLS домена и используют VLAN. В данном

примере можно использовать «чистую» установку; однако, они не ограничиваются только одним протоколом OpenFlow. Другими словами, OpenFlow контроллер способен получать и обрабатывать информацию, а также конфигурировать end-to-end сеть.

Та же миграция end-to-end сети, может быть пересекаться с различными вариациями сетевых сегментов и технологий. Например, сервис телефонии может пересекаться с многообразием сетей и различных технологий. Каждая технология может быть включена через OpenFlow, но фактически возможен перевод целиком различных технологий.

Рисунок 6 иллюстрирует такое распределение, где конечные пользователи мобильных устройств подключаются к уровням доступа, метро и ядрам сети, в конечном итоге к центрам обработки данных. Данная иллюстрация предлагает такое развертывание, которое будет включать серию из смешанного или гибридного внедрения. В некоторых случаях будет включена «чистая» установка, но это менее вероятно для end-to-end сети.

### 1.3 Типы сетей.

Работа по миграции должна рассматривать и учитывать 4 основных категорий сетей: Кампусные, Корпоративные Центры обработки данных, Распределенные центры обработки данных и Сервис Провайдеры или WAN. Каждый из этих типов имеет свои различные подтипы.

- Кампусные сети обычно располагаются в нескольких зданиях, каждое из которых имеет сетевой шкаф. Здания соединены с центральным операционным центром. Компоненты Кампусной сети включают магистраль с точкой подключения к глобальной сети (WAN), которая обычно связана с центрами обработки данных. Во многих случаях сети будут включать логические разделения – различные департаменты, административные деления или кампусные ИТ ресурсы.
- Корпоративные Центры обработки данных (ЦОД) могут различаться по размерам, но обычно рассматриваются сетевые ресурсы, используемые между различными подсетями серверов (физические или виртуальные), совместно с хранением (такие как Network Attached Storage (NAS) или Storage Area Network (SAN)), безопасность и сетевые функции (например, управление загрузкой). Требования для программно-конфигурируемых сетей могут различаться, но приложения управления сервисами имеет высокий приоритет.
- Распределенные ЦОДы получают большие преимущества от программно-конфигурируемых сетей. Эти ЦОДы имеют те же аспекты, что корпоративные ЦОДы, однако, распределенные должны обмениваться физическими ресурсами. Виртуализация вычислительных ресурсов – практическая необходимость; высокая доступность при миграции виртуальных машин, включающая в себя балансирование ресурсов, управление производительностью и отказоустойчивость. Программные коммутаторы внутри вычислительных ресурсов являются доминирующим компонентом архитектуры. Как следствие,

преимуществом является то, что части ЦОДов возможно перемещать и изменять. Все чаще, однако, программно-конфигурируемые сетевые устройства обеспечивают данные требования.

- WAN/Сервис Провайдеры/Сети Оператора Связи являются самыми разнообразными. Архитектура сети сервис провайдера и требования очень различны. Например, оператор мобильной связи будет иметь радиовещательную сеть вместе с мобильными транзитными сетями, которые не касаются к уровню доступа сети и в конечном счете ядра сети. Различные приложения OpenFlow и SDN разработаны и разрабатываются. Сервис провайдеры используют OpenFlow для управления обменом ресурсами, например, Google для глобально распределенными соединениями между ЦОДами, обеспечивая надлежащую полосу пропускания в текущий момент времени. Стоит отметить, что это подобно наложению сети по типу приложения. Много других примеров разработки в индустрии с помощью программно-конфигурируемых решений адресаций от уровня 0 до 7 сетевой модели.

### 1.4 Сетевые уровни.

Помимо разделения на типы сетей, существует еще слои сети. Изначально целевая архитектура и возможности OpenFlow были основаны на 2 уровне управления потоком сетевой модели передачи данных. Однако, OpenFlow эволюционировал и стал включать в себя уровни: 0, 1, 2, 2.5, 3, 4; и даже 7 уровень. Различия в уровне передачи (data plane) и уровне управления (control plane) требуют соответствующих рекомендаций по миграции.

Стоит рассмотреть определенное ранее гибридное устройство. Оно является сетевым устройством, которое способно быть управляемым OpenFlow контроллером, но также оно способно быть самостоятельным в управлении (Control Machine). Если вникнуть в действующие сети, то можно найти там устройства, которые способны работать на нескольких уровнях. На рисунке 11 изображены такие комплексные сети, где могут быть перенесены отдельные слои или группа слоев сетевой модели.

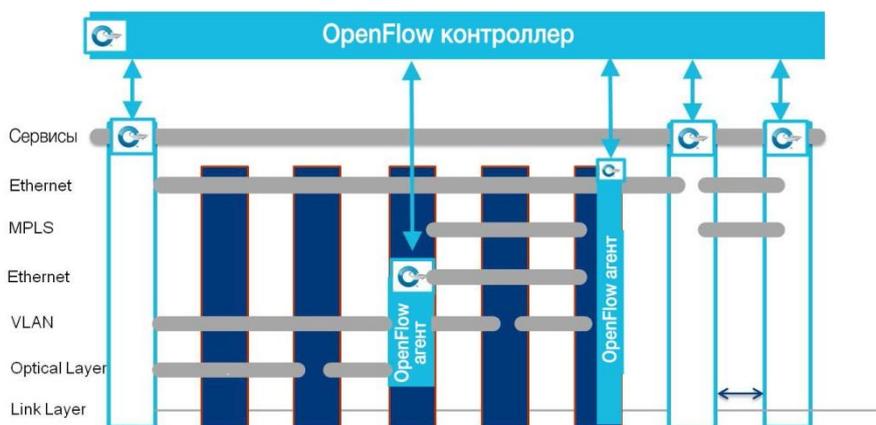


Рисунок 10 – Пример различия слоев при миграции.

Рисунок 10 отображает каждое физическое сетевое устройство, участвующее в end-to-end сети. Оборудование А, например, обеспечивает соединения на 0 уровне, но завершает оптический сигнал вводя значения в нагрузочную информацию VLAN/Ethernet в Lambda (многопротокольные коммутации в оптической сети). Такое устройство рекомендуется, если на уровне передачи данных OpenFlow используется Lambda.

Оборудование В – это обычный оптический коммутатор, где сигналы или нагрузочная информация не завершаются (например, аналоговые технологии). Оборудование С – это Оптико-электрический коммутатор (Optical-Electrical), которые просто восстанавливают заголовок VLAN для передачи в другой VLAN.

Оборудование D является шлюзом широкополосной сети. Это устройство может работать в различных слоях сетевой модели. Чаще всего оно действует на первых трех уровнях внутри сети и будет подключенным к Ядру сети (часто основан на MPLS).

Оборудование E является промежуточным коммутатором или скорее MPLS устройством, которое использует Label Switched Path (LSP). Устройства F и G являются MPLS коммутаторами, которые или перенаправляют LSP, или оканчивают LSP.

Наконец оборудование H – Ethernet устройство, которое может распознать только Ethernet фреймы, приходящие на порт.

### 1.5 Возможные сценарии миграции.

Три наиболее вероятных сценария миграции:

- Миграция А – Точка-точка (End-to-end) миграция: иллюстрирует точка-точка «чистую» миграцию со всеми устройствами, работающими на том же уровне (уровнях). Все устройства заменены на OpenFlow устройства и управляются через OpenFlow контроллер.

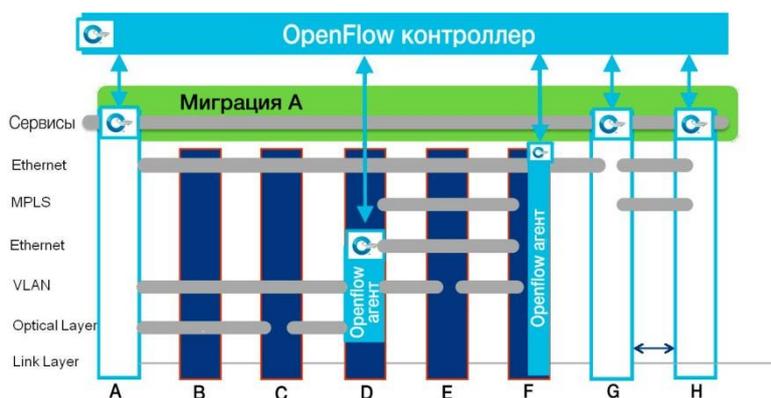


Рисунок 11 – Пример миграции точка-точка.

- Миграция В – Миграция с Full-Stack передачей: Оборудование F в этом примере является отражением гибридного оборудования (как описано выше), тогда как устройство G – полностью OpenFlow. Устройство F будет еще обмениваться инфор-

мацией с самоуправляемым устройством, но в то же будет использовать команды от OpenFlow контроллера. Это пример Гибридной миграции.

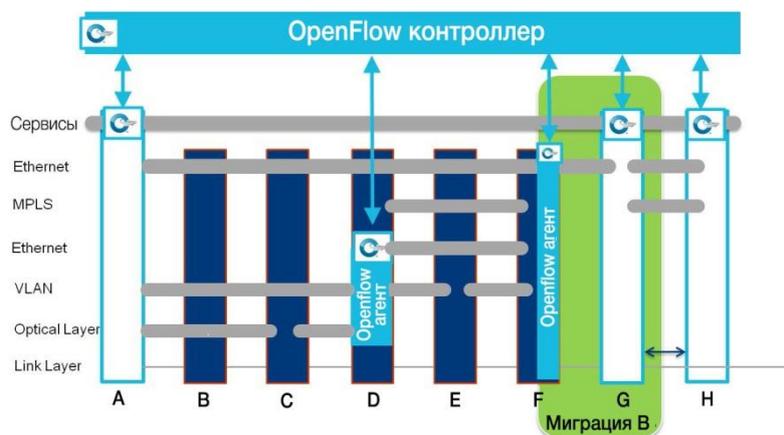


Рисунок 12 – Пример с Full-Stack передачей

- Миграция С – частично-заменяемая стек: Только несколько уровней сетевой модели будет перенесены на OpenFlow (Ethernet, VLAN и оптические уровни), где уровни выше и ниже (MPLS и Ethernet) могут продолжить использовать существующий управляемый механизм и протоколы, но выбранные уровни будут заменены OpenFlow.

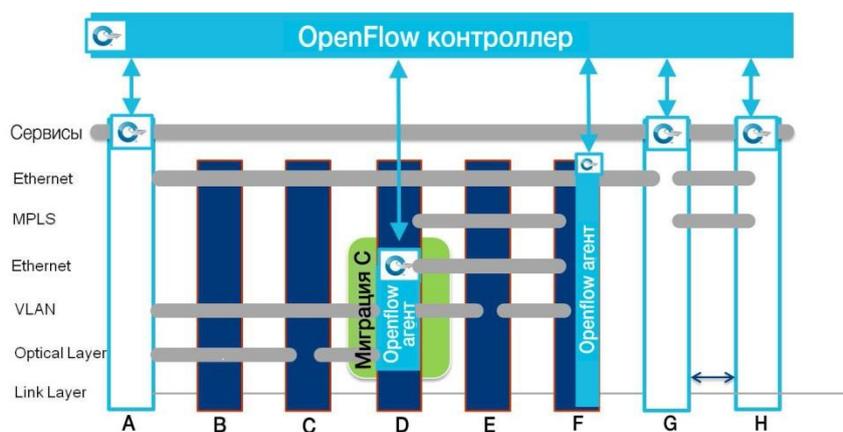


Рисунок 13 – Пример использования частично-заменяемого стека миграции.

## 1.6 ПКС архитектура по развертыванию сервисов.

OpenFlow – основанное на ПКС развертывание, будет включать один или более OpenFlow поддерживающих устройств, управляемых логически-централизованным контроллером и агентом. Физически, контроллер и агент могут осуществляться на серверах или встроенными внутри некоторых или всех OpenFlow устройств. Выбор архитектурных решений делается в соответствии с индивидуальными потребностями, полностью задокументированными.

Кроме того, характер трафика между контроллером и агентом может накладывать различные требования по развертыванию. Например, контроллер и агент могут использовать резервные запросы. Это могут быть редкие или частые (например, VM миграция внутри ЦОД) запросы. Трафик между контроллером и агентом может включать сигнальные протоколы, которые не могут быть мигрированы на OpenFlow, такие как Dynamic Host Configuration Protocol (DHCP), Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Internet Protocol Television (IPTV), 3GPP и т.д. К планируемым мощностям необходимы требования устойчивости и надежности. В случаях, где 100% трафика должно быть направлено к контроллеру, то необходимо предъявить особые требования к планированию передачи данных и соединения (например, если передающее устройство может пропускать 1ТБ трафика и 100% трафика будет обслужено, то использование 10 Гб соединения будет недостаточным).

Наконец, все возможные типы трафика к программно-конфигурируемой сети должны быть рассмотрены. Например, если тип трафика – голосовой, то требования будут отличаться от мультикаст видео или обычным трафиком данных.

## **1.7 Безопасность.**

Безопасность сетей является критическим звеном для всех бизнесов, особенно учитывая рост миграции к облачным вычислениям и программно-конфигурируемым сетям. ПКС обеспечивает централизованность и управляемую модель, что позволяет сети быть более гибкой и отразить атаки на сеть. ПКС может управлять сетью на основе анализа трафика и статистики и применять различные политики безопасности, а также определение источник атак и дальнейшее изолирование части сети.

Один способ безопасной миграции к ПКС:

- 1) Добавить экспериментальный слой сети (например, VLAN).
- 2) Ограничить этот слой с ПКС решениями по безопасности (например, Security Enhanced Floodlight).
- 3) Включить OpenFlow и решения по безопасности ПКС на новом слое сети (например, VLAN).
- 4) Поэтапно переводить пользователей к новому безопасному слою.

## **2. Успешные примеры миграции.**

В данной части будут выделены основные тезисы по миграции, которые были выделены из анализа сделанных миграций. На данный момент состоялись следующие успешные миграции:

- 1) Google Inter-Datacenter WAN;
- 2) NTT Provider Edge;
- 3) Stanford Campus Network.

Цель данной части ограничить нарушения сети и оставить сервисы доступны во время миграции сети к ПКС.

## 2.1 Планирование.

Успешная миграция возможно при правильном планировании, где лучшими рекомендациями будут:

- Анализ несоответствий: детальный анализ несоответствий должен выполняться для понимания влияния на существующие сервисы. Для всех несоответствий (промежутков времени) необходимо обеспечить альтернативные варианты доступности для предотвращения возможных ошибок, которые могут возникнуть в течение миграции.
- Чек-лист: перед и после миграции необходимо заполнить чек-лист, в котором указаны специфичные особенности.
- Процедуры возврата: детальное описание миграции шаг за шагом с описанием процедуры возврата на предыдущий этап. Это должно быть полностью задокументировано для действий в случае непредвиденных результатов. Также возврат должен быть минимизирован для запроса ресурсов производительности.
- Анализ набора особенностей: детальный анализ OpenFlow особенностей и желаемых возможностей должны быть выполнены на контроллере и OpenFlow коммутаторе. Необходимо обеспечить набор особенностей в соответствии с требованиями.

## 2.2 Процесс миграции.

Следующие практики являются важными для плавного хода миграции:

- 1) Инструменты. Все необходимые инструменты управления сетью должны быть резервированы для правильного управления и мониторинга трафика.
- 2) Управление контролем версий OpenFlow. Так как есть несколько версий OpenFlow, то важно проверить совместимость между версиями OpenFlow протокола в контроллере и коммутаторах.
- 3) Обновления. OpenFlow устройства должны быть обновлены для запуска соответствующего кода, и произведена аппаратная прошивка перед процессом миграции.
- 4) Соединения. Каналы связи между контроллером и OpenFlow коммутаторами должна быть проверена.
- 5) Доступность сервисов. В смешанных сетях вспомогательные инструменты, такие как VPN, должны быть созданы и проверены.
- 6) Поиск ошибок. Соответствующие шаги по поиску ошибок и проблем, такие как ping, trace, должны быть проверены.

## Заключение.

В данной статье были рассмотрены методы для миграции сети от традиционной архитектуры к программно-конфигурируемой сети на основе OpenFlow. Традиционные сети

включают Традиционные сети охватывают самые различные области, включая WAN/сети сервис-провайдера/ сети оператора связи, сети центров обработки данных, корпоративные сети и кампусные сети. Данная работа также фокусируется на успешных ПКС миграциях и в конце приведены основные тезисы и рекомендации по методам миграции, инструментам и системам.

Данная статья может рассматриваться как основа для методов по миграции. Здесь определены и даны определения целевой сети, требований ядра сети, исходной сети, требования к миграции, этапы миграции и наконец проверка требований для обеспечения полной и успешной миграции.

Одной из основных целей перехода к ПКС является получение новых сервисов. Эти сервисы могут быть точка-точка, поверх сети (виртуальная сеть), несколько сетевых сегментов и/или несколько уровней сетевых технологий. OpenFlow может использоваться на уровнях 0, 1, 2, 2.5, 3, 4-7. К статье были добавлены данные из примеров: Google Inter-Datacenter WAN; NTT Provider Edge; Stanford Campus Network.

Данную работу стоит продолжить в дальнейшем, например, на этапе текущего планирования добавить: инструменты по миграции и метрики, прототипы миграции, симуляторы сети и программное обеспечение по управлению производительностью.

### Список литературы

1. Смелянский Р Программно-конфигурируемые сети//Открытые системы. 2013.URL: <http://www.osp.ru/os/2012/09/13032491/> (дата обращения: 01.11.2013).
2. Thomas D. Nadeau, Ken Gray, SDN: Software Defined Networks, O'Reilly, 2013. pp 10-25.
3. OpenFlow Tutorial//OpenFlow.2013.URL. // [http://archive.openflow.org/wk/index.php/OpenFlow\\_Tutorial](http://archive.openflow.org/wk/index.php/OpenFlow_Tutorial) (Дата обращения: 07.11.2013).
4. ONF Specification//Open network foundation.2013.URL: <https://www.opennetworking.org/sdn-resources/onf-specifications> (дата обращения: 07.11.2013).
5. Onix: A distributed control platform for large-scale production networks /Т. Koponen [и др.], OSDI, 2010. 14 p.
6. Andrea Dainese Route Reflector 2013. URL. <http://www.routereflector.com/en/2013/11/natively-l3-routing-using-sdn-pox-controller/> (Дата обращения: 07.11.2013).
7. ONF Specification//Open network foundation.2013.URL. <https://www.opennetworking.org/sdn-resources/onf-specifications> (дата обращения:07.11.2013)