Руслан Смелянский – директор Центра прикладных исследований компьютерных сетей (НП «ЦПИКС»), д.ф-м.н., Профессор МГУ им. М.В. Ломоносова, член-корреспондент РАН.

SDN&NFV – новые горизонты

Введение

Вот уже на протяжении четырех лет мы наблюдаем, как меняется ландшафт ИКТ (информационно-коммуникационной инфраструктуры) под влиянием технологий SDN и NFV. Смещение акцента со специализированного аппаратного обеспечения для middlebox на commodity железо с активным использованием программного обеспечения существенно меняет приоритеты в телекоме, в ЦОДах, в корпоративной сети.

Одним из характерных знаков этих изменений является переход к виртуализированным системам: компании сокращают количество и масштабы серверной и сетевой инфраструктуры. Так, по информации IDC совокупный рынок сетевого оборудования, серверов и внешних систем хранения данных будет расти в ближайшие пять лет среднегодовым темпом 0,1%, тогда как поставки конвергентных систем сетевого оборудования, серверов и внешних СХД аналогичной функциональности в виде виртуализированных сетевых сервисов − 19,6%. По данным того же IDC, затраты на публичные облачные (операционные) услуги в мире приблизятся в 2016 году к $100 млрд. Для примера, в 2009 году доходы от облачных вычислений составили $ 5860 млрд, а в 2013 году они увеличились в более чем в два раза и составили $ 13,070 млрд.

Если еще три года назад ИТ- сообщество в России путало понятия ISDN (Integrated Services Digital Network, цифровая сеть с интегрированным сервисом) и SDN (Software Defined Networks, программно-конфигурируемые сети), то сегодня специалисты (конечно те, кто знают, что такое ISDN) четко понимают разницу не только между ними, но и между SDN и NFV (Network Function Virtualization, виртуализация сетевых функций). Из-за геополитических событий аббревиатура SDN теперь знаком многим – так США называют санкционные списки (Specially Designated Nationals), но это уже другая тема. Хотя, проблема импортозамещения и появление технологий SDN и NFV на рынке, удачно совпали для нашей страны. С ними нам не надо никого догонять, необходимо, не теряя темпа, встраиваться в идущий процесс.

Изменения, вызванные появлением этих технологий и их конвергенцией, затронули не только индустрию ИКТ, но и вызвали кардинальные изменения бизнес-процессов. Так, психология «трубы» в телекоме уходит в прошлое. Представители нового подхода в бизнесе говорят: «денег с клиентов за доступ не надо брать». Доступ к «трубе» должен быть бесплатным, платным должен стать контент и услуги. Базовая идея Google или Apple - брать деньги не за коннект, а за доступ к клиентам и информации о них. Эти компании уже пытаются разными технологическими способами отодвинуть операторов связи от клиентов. Информация о клиенте и доступ к нему – вот, что сейчас на вес золота и дороже барреля нефти. Одним из первых свои силы здесь попробовала компания AT&T.

В 2011 году этот оператор запустил подразделение AdWorkds, с помощью которого рекламодатели могли получить доступ к данным пользователей. В мае 2013 года AdWorks запустила платформу Blueprint, с помощью которой рекламодатели могли получать доступ к анонимизированным данным 70 млн пользователей для целенаправленных рекламных кампаний в вебе, мобильной среде и на ТВ. В октябре 2012 года о запуске инициативы Precision Market Insights объявил другой оператор — Verizon. В рамках этой инициативы рекламодатели могли получить доступ к данным пользователей мобильной связи для повышения эффективности наружной и онлайн-рекламы. О запуске собственной рекламной биржи в апреле 2014 года объявил испанский телеком-оператор Telefónica. Компания объединила усилия с инвесткомпанией Blackstone и выкупила технологию обанкротившейся биржи MobClix. В результате была создана новая компания Axonix, которая будет выступать в роли посредника между рекламодателями и интернет-площадками во всем мире, при этом ключевыми рынками называются США, Европа и Латинская Америка.

Мы видим, что наиболее доходными форматами для бизнеса становятся конвергенция сервисов и конвергенция данных. Это требует технологий, которые позволят динамично управлять потоками данных, менять состав и расположение сервисов внутри сети, обеспечить пользователю возможность унифицированного доступа к сервисам независимо от его географического местоположения, используемого оборудования и способа подключения к сети, конечно же, при условии достаточной пропускной способности канала.

Главным условием успеха ИТ-бизнеса XXI века становится скорость адаптации к изменениям рынка. Цель данной статьи – показать синергию технологий SDN и NFV, то, как под их влиянием происходит конвергенция в ИКТ инфраструктуре, и те горизонты, которые открываются.

Синергия SDN и NFV

Технологии программно-конфигурируемых сетей (SDN) и виртуализации сетевых функций (NFV) возникли независимо друг от друга. Более того, они зародились в разных отраслях ИКТ индустрии.

Компании и консорциумы, занимающиеся разработкой решений SDN, являются по сути своей традиционными IT компаниями. Например, NEC, HP, Cisco, Huawei, Extreme Networks, IBM, Brocade, BigSwitch Networks, Juniper. Можно так же перечислить целый ряд отечественных компаний, проявляющих повышенный интерес к этим технологиям. По своей воле, или подчиняясь требованиям рынка, они вкладывают существенные средства в стандартизацию протоколов, эксперименты и поддержку немалого сообщества программистов, занятых в разработке различных SDN-приложений. Целью всех этих мероприятий является создание сетей нового поколения и тот, кто сумеет убедить рынок в перспективах своего видения развития, тот и получит значительную долю рынка.

Основными драйверами развития технологий NFV всегда являлись телефонные компании, операторы связи и провайдеры доступа. Например: NTT,

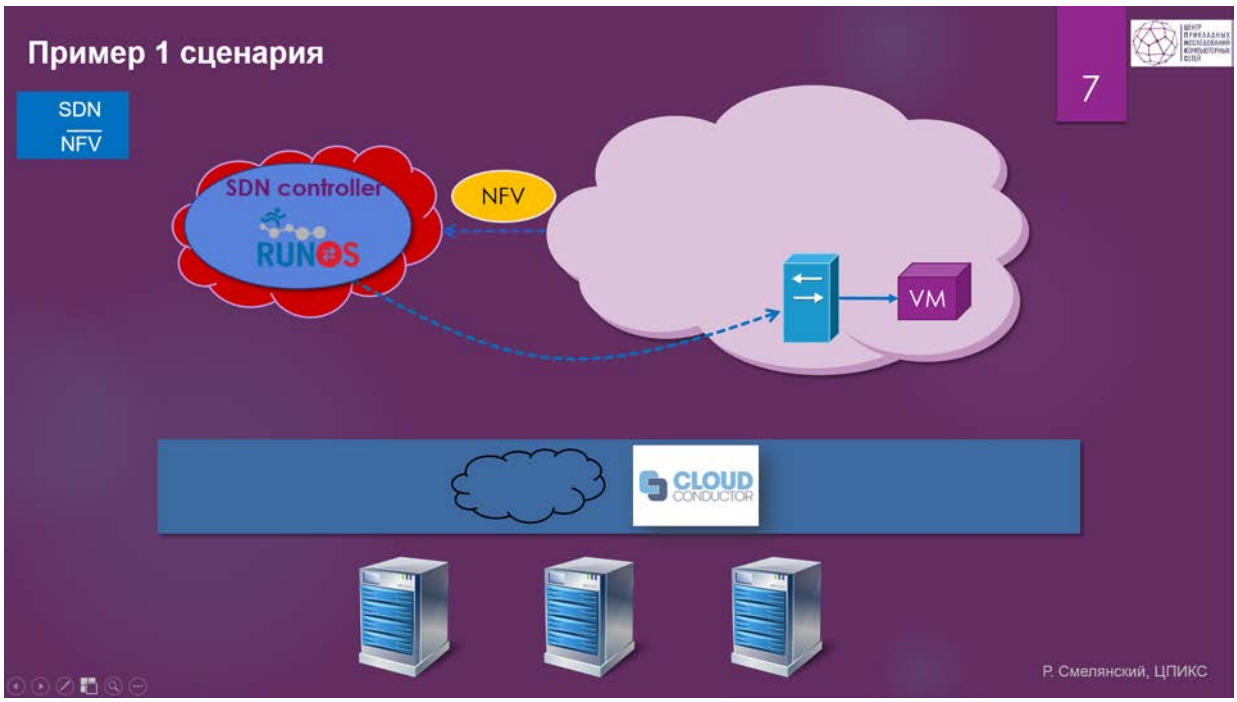
Telefonica, Deutsche Telecom, AT&T, Allot communication, Sonus networks, Sandvine, Contextream, Nuagenetworks. Подход этих компаний всегда был крайне прагматичен. Их интересуют сокращение ROI, возможность оперативно откликаться на требования клиентов. Всем этим компаниям чрезвычайно интересна возможность использовать вместо дорогостоящих «middlebox» недорогие виртуальные машины, расположенные на обычных серверах в ЦОД. Это позволяет увести такие сервисы как BRAS, FireWall, IMS, DPI, CDN в «облако» и, при наличии облачной платформы, сделать это облако управляемым, масштабируемым.

Идея составить конкуренцию сетевым «монстрам», производящим дорогостоящие «middlebox», витала в воздухе давно, однако разработчиков сдерживали два существенных момента. Первый – сетевой стек Linux не позволял обрабатывать пакеты на скорости интерфейса в режиме коммутация/маршрутизация. Это было вызвано логикой работы классической ОС, которая обязана поддерживать все возможные сетевые протоколы для конечных систем. Второй момент заключался в том, что даже при попытке обойти сетевой стек, разработчик упирался в производительность центрального процессора. В результате для обеспечения нормальной работы интерфейсов уходило недопустимо большое количество ядер процессора. Производители сетевых «middlebox» использовали модифицированные, специальным образом доработанные ОС для решения этих проблем. Конечно, широкой программистской общественности эти разработки были не доступны.

Это не могло продолжаться вечно и, пару лет назад, ситуация революционным образом изменилась. На рынке появилось достаточное количество Open Source продуктов, позволяющих решить проблемы реализации сетевых функций, таких как Межсетевой Экран, системы предотвращения вторжений и т.п., на обычных серверах. Это продукты OpenvSwitch, Data Plane Development Kit ®Intel, NetMap, Lagopus, QEMU. Список далеко не полон, но он дает нам возможность осознать тот факт, что используя открытые продукты, можно самим создавать и виртуализировать сетевые сервисы. При этом сервисы смогут работать на скоростях близких к скорости физического интерфейса.

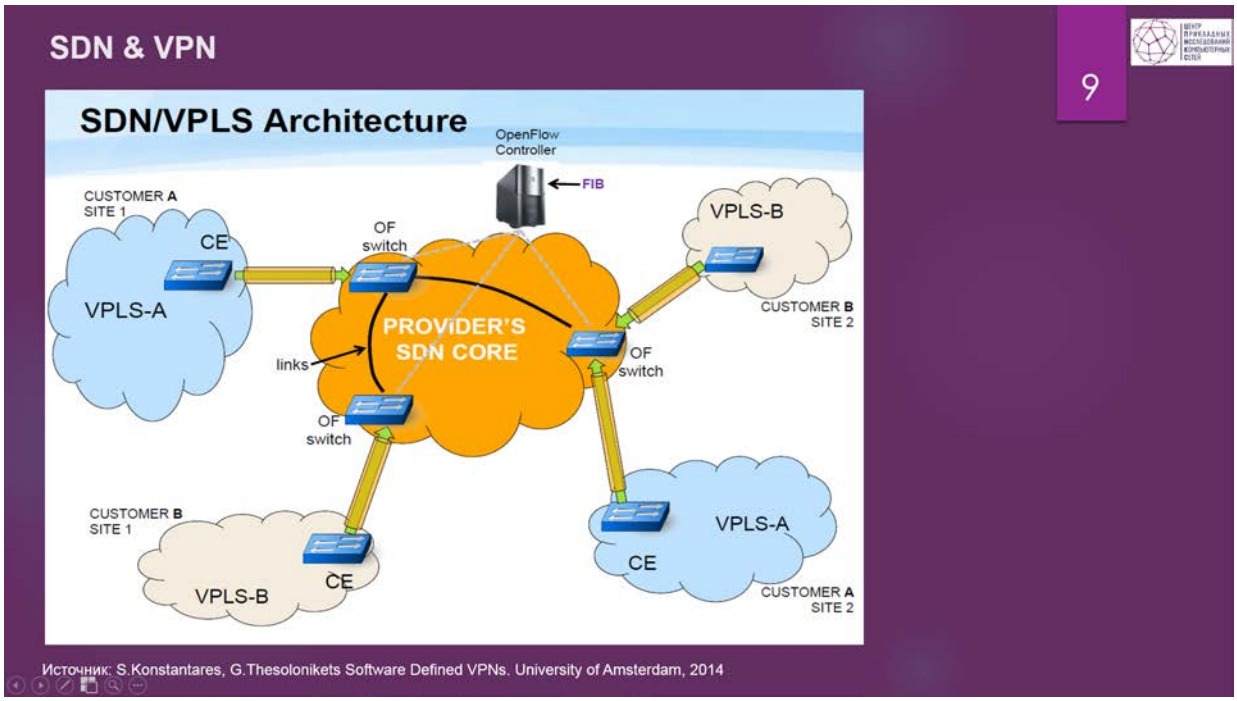
Таким образом, технологии SDN и NFV развивались параллельно, особо не обращая внимания на возможности друг друга.

Многие разработчики в настоящее время начали эти две технологии использовать одновременно. Самый простой пример: SDN-контроллер является программным обеспечением, выполняющим классическую сетевую функцию – управление коммутаторами. Его можно запустить на обычном сервере, но зачем это делать, когда мы можем функциональность управления SDN коммутаторами виртуализировать, поместить в «облако». В результате мы получили симбиоз SDN и NFV. (См. рис.)



Рассмотрим вариант посложнее. Представьте себе сеть оператора, который предоставляет услуги организации VPN L2 для предприятий. В настоящее время эту услугу реализуют с помощью решения MPLS/VPLS. Для этого необходимо сначала спроектировать виртуальную сеть, потом настроить все сетевые устройства. Эта задача требует серьезной квалификации персонала и времени. Мы можем виртуализировать функцию проектирования VPLS туннелей с помощью несложного графического интерфейса, а настройку коммутаторов моментально произведет SDN контроллер.

(См. рис.)



Теперь мы можем создавать целые цепочки сервисов для различного вида трафика. Мы встраиваем мощный сервер с платформой поддержки и управления виртуализированными сервисами (NFV) в инфраструктуру сети, управляемой SDN контроллером. Это позволяет управлять цепочками сервисов не только проактивно, но и реактивно, динамически.

Пример. Проактивное правило «весь трафик, следующий на адреса партнера X.X.X.X должен сначала пройти шифрацию на NFV сервере». Реактивное правило «В случае если приложение IDS на контроллере подозревает аномалию в трафике пользователя Y весь его трафик перенаправить на виртуализированную систему противодействия вторжениям (IPS NFV)». В результате мы получаем сеть, которая динамически меняет маршрутизацию трафика по событиям.

Последнее время производители SDN коммутаторов стали обращать свое внимание на возможность использования т.н. сетевых процессоров (например NP-4,NP-5, NPS-400). В этом случае можно часть сетевых функций (Шифрация, DPI,Туннелирование, NAT…) реализовать прямо на интерфейсах, «смотрящих» на оператора .

Сочетание виртуальных сетевых функций (VNF) и реальных высокоскоростных сетевых процессоров позволит создать очень эффективное и производительное решение, которое потенциально не имеет ограничений по наращиванию функциональности.

Безопасность в SDN

SDN- сети имеют две особенности, которые могут быть привлекательны для киберпреступников, и также будут головной болью для менее подготовленных сетевых администраторов. Первое, это возможность управлять сетью с помощью программного обеспечения (часто имеющего ошибки и уязвимости). Второе, это централизованное управление сетью из контроллера. Любой, у кого есть доступ к серверам, хранящим в себе управляющее программное обеспечение, может потенциально контролировать всю сеть.

Ниже приведен список возможных атак, которые специфичны для SDN-сетей:

- Искажение данных
- Раскрытие информации о состоянии и статусе сети
- Отказ в обслуживании
- Компрометация коммутатора
- Перехват трафика;
- Атака на канал управления

Рассмотрим, в качестве примера, основные атаки на канал управления, которые возможны при компрометации коммутатора.

Перехват управляющего трафика

Атакующий может использовать скомпрометированный коммутатор для перехвата управляющего трафика, идущего через данный коммутатор в том случае, если не используется TLS.
Более того, атакующий может перехватывать управляющий трафик, посылаемый скомпрометированному коммутатору, если перед этим был произведен перехват управляющего канала. TLS защита не сможет противостоять данной атаке в случае, если атакующий способен извлекать криптографические ключи из скомпрометированного коммутатора. Основным методом защиты от подобных атак является использование out-of-band передачи управляющего трафика.
Скомпрометированный коммутатор может быть использован для атак на целостность сети. Атакующий может производить подделку видимого для контроллера состояния коммутатора. Такая атака называется – подделка состояния коммутатора. Если в сети не используется протокол TLS или он используется только для аутентификации контроллера, атакующий может создавать поддельные виртуальные коммутаторы в данной сети. Подобная атака называется – подделка состояния сети.

Подделка состояния коммутатора и сети

Скомпрометированный коммутатор используется атакующим для того, чтобы передавать контроллеру ложные сведения о текущем состоянии данного коммутатора или других коммутаторов, которые подключены к контроллеру через скомпрометированный коммутатор. Например, атакующий может передать контроллеру ложную информацию о содержимом таблиц потоков, о статистике по трафику или даже о том, какие интерфейсы имеет коммутатор. Атакующий может использовать подобные атаки для сокрытия своих действий от контроллера.
Кроме того, атакующий может подделывать состояние других коммутаторов в случае, если в сети не используется TLS. Данная угроза показывает важность использования аутентификации в SDN сети. Стоит отметить, что даже если TLS используется только для аутентификации контроллеров, атакующий будет не способен произвести MitM атаку на управляющий трафик, проходящий через скомпрометированный коммутатор. Однако, если TLS не используется для аутентификации коммутаторов, то атакующий сможет создавать поддельные коммутаторы в сети. Данная атака может быть использована для изменения сетевой топологии, которая хранится у контроллера. Создавая поддельные коммутаторы, атакующий может влиять на процесс выбора маршрута для потоков в сети.

Компрометации контроллера

Приложения, работающие на контроллере, могут содержать в себе уязвимости, эксплуатация которых приведет к компрометации контроллера атакующим. Также

приложения могут уже содержать в себе вредоносный код, если они были загружены от непроверенных производителей.
Большинство современных контроллеров не предоставляют разграничение доступа для приложений на контроллере, что приводит к тому, что каждое приложение может иметь доступ не только к внутренним данным других приложений, но и к внутренним структурам контроллера (например, к внутреннему представлению сети). Также многие контроллеры не производят контроль ресурсов, запрашиваемых приложениями. Это происходит из-за того, что в контроллерах, для повышения производительности, приложения реализуются в виде библиотек, которые загружаются в адресное пространство контроллера.
Типичной атакой, базирующейся на данных свойствах контроллеров, может быть то, что вредоносное приложение может изменить структуру, содержащую внутренне представление сети, что приведет к неправильной работе всех приложений на контроллере.

Конвергентные сети

Термин конвергенция уже много раз встречался в этой статье. Объяснить, что такое конвергентная сеть лучше всего на сравнении с мультисервисными сетями. Последние достаточно широко вошли в нашу жизнь и хорошо понимаются многими. Мультисервисная сеть предполагает унификацию коммуникаций, которая обеспечивает передачу данных, не зависимо от сервиса, нужный уровень QoS, позволяет выбирать среду коммуникации в зависимости, например, от величины задержки, имеет возможность управления всеми потоками данных в рамках единой системы управления.

С точки зрения потребителя важным достоинством мультисервисных сетей является возможность передачи данных на базе самых разных каналов, имеющихся у телекоммуникационных провайдеров. Тем самым они получают возможность повысить количество сервисов, используя имеющуюся инфраструктуру и не производя при этом вложений в ее модернизацию. Мультисервисные сети сегодня могут работать и работают поверх протокола IP, что обеспечивают IP-коммутаторы для мультисервисных сетей. Это объясняется тем, что мультисервисные сети, соединяющие удаленные офисы и территориально распределенных клиентов, просто вынуждены работать, используя каналы Интернета, что обрекает их на коммутацию поверх протокола IP. При этом одной из основных задач мультисервисных сетей является оптимизация использования полосы пропускания и гарантии QoS для чувствительных приложений на базе даже не слишком быстрых каналов.

В конвергентных сетях уже не решают таких задач, как экономия полосы пропускания в чистом виде, и это вполне объяснимо, ведь скорости постоянно растут, а тарифы на передачу данных дешевеют. Конечно, в рамках конвергентной сети также возможна оптимизация трафика, изменение качества передачи того же голоса, но это уже не первоочередная задача.

Основное отличие конвергентной сети от мультисервисной - это возможность оперативно изменять состав и расположение сервисов, действующих внутри сети, а также обеспечить пользователю возможность унифицированного доступа к сервисам независимо от его географического местоположения, используемого терминала (smartphone, tablet, desktop etc.) и способа подключения к сети, конечно же, при условии достаточной пропускной способности канала. Поэтому понятие конвергентности можно рассматривать применительно к любым аппаратно-программным платформам, которые обеспечивают единообразный доступ к различным приложениям и сервисам. Хорошим примером здесь является система Skype, которая позволяет через один и тот же интерфейс поддержать общение в чате, телефонный звонок, видеоконференцию. Тем самым, если пользователь устанавливает Skype у себя на desktop, на ноутбуке и карманном компьютере, а также настраивает переадресацию на сотовый телефон, он получает доступ к конвергентным коммуникациям в рамках системы Skype.

Помимо удобного пользовательского интерфейса конвергентные сети должны поддерживать сразу несколько уровней функционирования инфраструктуры. Среди них обязательно должна присутствовать система обеспечения безопасности, надежная сеть передачи данных, широкий набор коммуникационных сервисов, которые обеспечивают адекватный QoS для разных типов, данных на разных уровнях (Layer 4-7). В дополнение к этому конвергентная сеть должна уметь взаимодействовать с разными видами терминалов, способных обращаться к сервисам и приложениям (smartphone, PC, активные сетевые устройства), а также единую платформу управления всем этим перечнем приложений, аппаратных средств и каналов передачи данных.

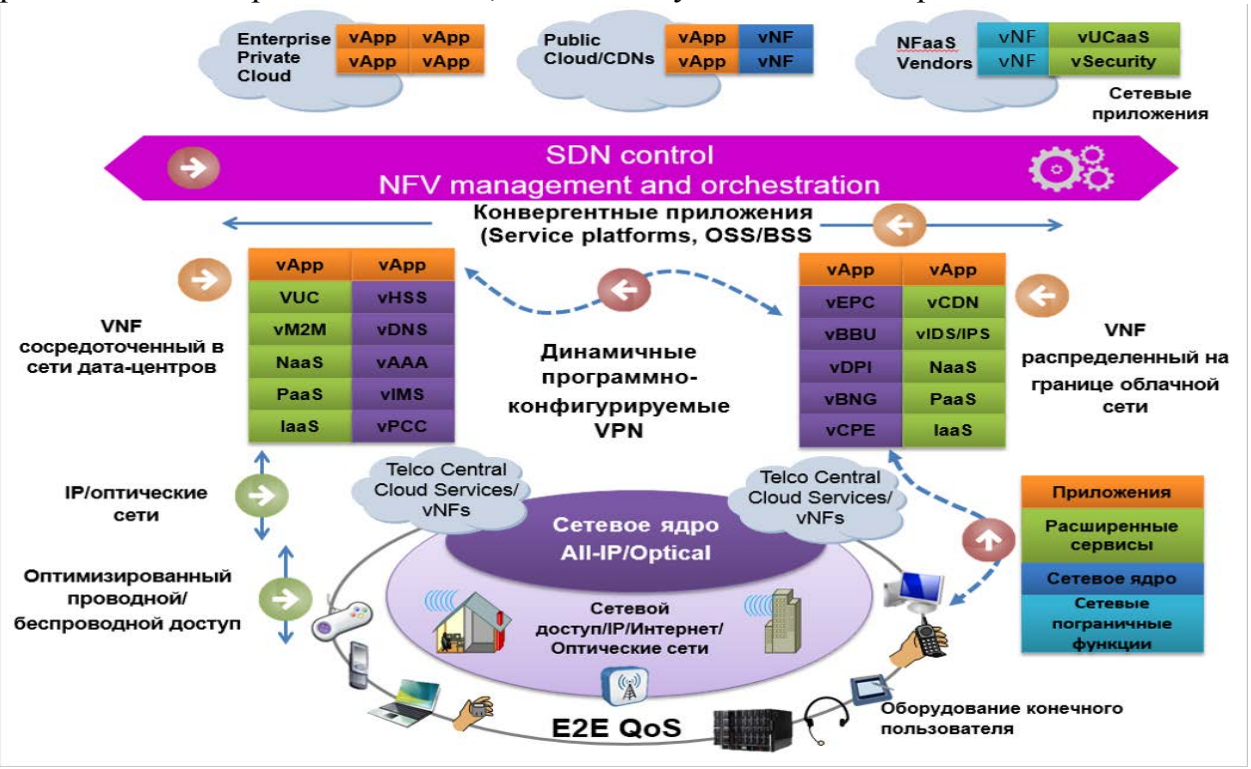
Конвергентная сеть должна уметь выбирать канал передачи данных в зависимости от требований QoS приложения. Когда речь заходит о передаче данных, всегда возникает вопрос о протоколе. Существует несколько вариантов: начиная с принципов общения в сетях, подобных Skype, где для инициации сессии и передачи данных используется частный протокол, и заканчивая открытыми мультимедийными протоколами (H.323 или SIP). Протокол H.323 успешно используется сегодня для организации IP-телефонии многими производителями, однако при его дальнейшем расширении возникают сложности, главный источник которых состоит в том, что H.323 прекрасно оптимизирован для IP-телефонии, но не для любых сервисов, в том числе мультимедийных. Кроме этого, описание формата сессии в H.323 требует использования специального формата, что усложняет адаптацию этого протокола для применения в конвергентных сетях.

Протокол SIP (Session Intiation Protocol) на сегодня, пожалуй, получил наибольшее распространение для организации мультимедийных сеансов. По сути это протокол прикладного уровня. Его главная функция – инициация сессии и обеспечение независимости приложения от конкретного транспорта. Не важно будет ли это TCP или UDP. Достоинство SIP состоит в том, что в данном протоколе не заложены какие-либо форматы сессий передачи данных - эти параметры описываются уже в самом запросе SIP, причем в текстовом режиме, что значительно упрощает коммуникацию новых приложений на базе SIP.

Данный протокол работает в паре с SDP (Session Description Protocol) протоколом, который описывает параметры сессии передачи данных, а также позволяет их изменять во время сессии. Это очень удобно для управления QoS, когда возникает необходимость оперативно понизить или повысить качество сервиса. Протокол SIP полностью оптимизирован для работы на TCP/IP стеке и позволяет рассматривать любой трафик как обмен данными между двумя пользователями в Интернете. Еще одна интересная особенность, которую следует отметить: SIP может ассоциировать с одним адресом сразу несколько клиентов, что очень удобно для организации видеоконференций и любых трансляций, в том числе и для совместной работы через Web.

Важно, чтобы используемый на прикладном уровне протокол позволял получать информацию о характеристике сеанса передачи данных уже на этапе его инициации. В этом случае система управления коммуникациями конвергентной сети может учитывая потребности приложений в пропускной способности, требования QoS и SLA, что весьма актуально для телекоммуникационных провайдеров. Такая сеть может в реальном времени модифицировать свое состояние, отдавая приоритет голосу или видео либо подбирая для этого потока данных оптимальные параметры качества, учитывая характеристики сети передачи данных, а также серверной инфраструктуры

Ниже на рисунке, взятом из исследовательского отчета «Reshaping the future with NFV and SDN» Bell Labs Alcatel Lucent (2015) отражены все вышеперечисленное. SDN контроллер и его приложения призваны обеспечить оперативное управление потоками данных, балансировку и все что связано с управлением потоками в сети. NFV management and orchestration, как раз, отвечает за динамику состава и размещения сервисов в сети, включая увязывание сервисов в цепочки.



Сети информации (Information Centric Networks)

Впервые об этих сетях заговорили после выступления Van Jacobson на International Conference on emerging Networking EXperiments and Technologies (CoNEXT) в декабре 2009 года. Это тот самый Jacobson, который разработал механизм медленного старта для протокола TCP, кто внес огромный вклад в создании алгоритмов управления перегрузками. Сегодня у этого направления есть несколько названий Content Centric Network, Information Centric Network, Named Data Network. Не вдаваясь в детали различий, мы здесь постараемся кратко охарактеризовать основные идеи и направления развития этой архитектуры сетей грядущих поколений.

Исторически сети создавались для разделения ресурсов, а не данных. Как следствие в модели всех современных сетей центральной является понятие хоста, у которого есть уникальный адрес, а основной моделью взаимодействия – взаимодействие точка-точка двух хостов. При этом, на уровне приложения/пользователя в модели указывается «что» надо, а на уровне сети необходимо указать «где/кто» должен выполнить. Установить соответствие между этими моделями сегодня требует огромных усилий.

Сегодня контент в сети – основной объект взаимодействия. Если мне надо обеспечить консистентность данных на разных устройствах, мне нужно воспользоваться специальными приложениями, настроить их, поддерживать, инициировать и т.д. Сегодня нельзя сказать сети: синхронизуй всегда такие-то объекты в сети. Если бы так можно было бы сделать, то не надо было бы специально заботиться о синхронизации своего ноутбука, iPad’a или iPhone. Можно было бы попросить синхронизовать свое хранилище информации по какой-то проблематике с какими-то объектами, связанными с исследованиями по этой проблематике. Таких примеров применения можно было бы привести множество.

Однако контент - непрозрачная сущность для сети. Отсюда много проблем с безопасностью. Добиться этой прозрачности сегодня требует огромных усилий. Сети сегодня предназначены для передачи данных, а не для работы с контентом/информацией.

Целями создания Content Centric Network создать простую, гибкую, архитектуру общего назначения для коммуникации такую, чтобы преодолеть проблемы современных сетей, таких как:

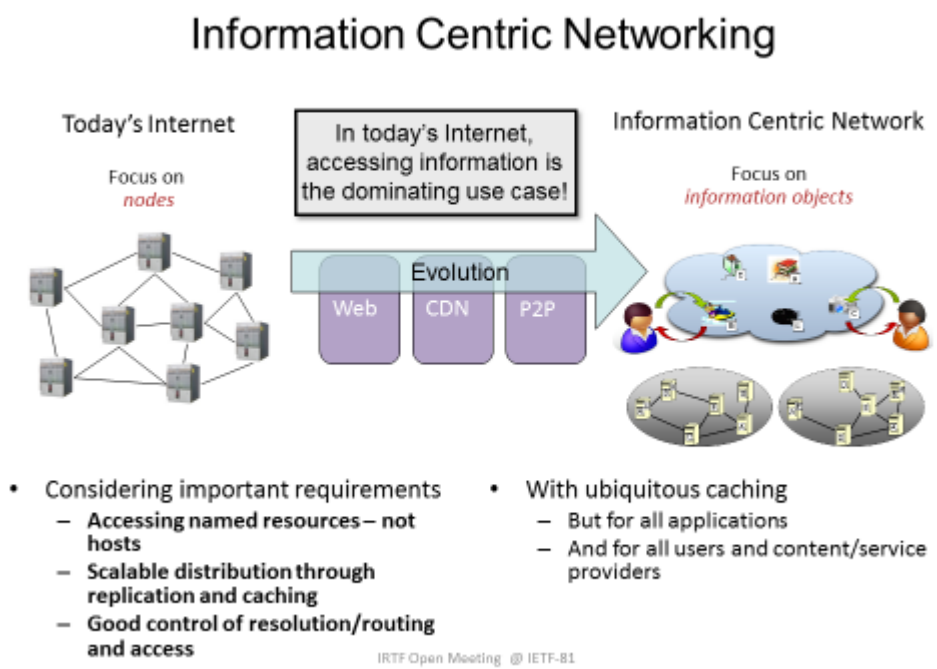
- Перегруженность механизмов именования данных URL, адресации IP и установления соответствия между ними;
- Перемещение сегодня информации в сети равносильно изменению имени, что недопустимо. Имя – это то, что идентифицирует объект, адрес – то, что указывает где находится объект;
- Нет надежного механизма поддержки идентичности копий. Отсюда проблема консистентности информации в сети;
- Нет эффективных механизмов распространения информации. Нет доступа к информации, хранящейся на локальных хостах. Нельзя найти ближайшую к Вам копию;

- Проблемы безопасности: нельзя доверять данным, полученным от неизвестного Вам хоста. Сегодня акцент на шифрование и доверенность серверов.

Information-Centric Networking (ICN) – это попытка отвязать Интернет от сложившейся парадигмы end-to-end соединения конечных точек в пользу адресации по «наименованию» контента или данных. Другими словами, адрес и имя в этих сетях будут одним и тем же. Данная парадигма предполагает сделать данные в сети независимыми от географического расположения за счет сетевого кэширования. Ожидаемые преимущества от использования данной парадигма: улучшенная эффективность использования сетевых ресурсов, масштабируемость и адаптивность к постоянно изменяющемуся поведению компьютерной сети.

Основной парадигмой Data Oriented Network Architecture (DONA) является парадигма publish/subscribe с разными вариациями. В этой парадигме есть два основных примитива: publish – опубликовать контент, т.е. сделать его видимым и доступным другим, и subscribe – объявить/запросить что Вам нужно.

Основой DONA является механизм кэширования контента, подобно тому как это сделано в CDN сетях (см. рисунок).



Источник IETF Information-Centric Networking Proposed IRTF RG, Dirk.Kutscher, Boerje.Ohlman

В ICN сетях, когда сетевой элемент получает запрос от себе подобного или хоста, то происходит одно из двух:

- Если в кэш у получившего запрос есть нужные данные, то он непосредственно отвечает на запрос;
- Если нужного контента нет в кэш, получивший запрос запрашивает себе подобных. Получив ответ, кэширует контент.

Это универсальный механизм, поскольку:

- Он применим к любому протоколу, не только специфическому для работы с контентом, но и для такого как HTTP. Тем самым он образует единый механизм кэширования, лежащий в основе доставки любого контента;
- Этот механизм пригоден для всех пользователей, а не только операторов CDN сетей. Он в этом смысле демократичен;
- Он должен поддерживаться всеми узлами в сети, а не только специализированными серверами, поэтому он призывает всю архитектуру DONA.

Особое внимание в DONA уделяется безопасности. ICN должна обеспечить безопасность контента, а не маршрут его доставки. Для этого используется content oriented модель безопасности, построенная на понятии реноме. В ICN контент ВСЕГДА подписывается поставщиком. Поэтому элементы сети, потребляющие контент, всегда могут определить его поставщика. Здесь основным вопросом безопасности становится вопрос безопасности имени контента в таких сетях. К решению этого вопроса есть два подхода. Первый – традиционный, на основе сертифицирующих серверов и PKI. Другой – когда само имя является ключом.

Следующей группой проблем является проблема маршрутизации по имени, и особенно междоменная маршрутизация.

Заключение

Итак, конвергенция технологий SDN&NFV привела к глубоким изменениям в ИКТ индустрии. Появилась возможность строить конвергентные сети, которые позволяют реализовать новые бизнес-процессы, строить новые бизнесы.

Разделение функций управления передачей данных и функций собственно передачи данных позволяет динамично управлять потоками в сети, автоматизировать многие процесса администрирования сетей, динамично менять состав и размещение сервисов в сети. Это, в свою очередь, кардинально менят и экономику, и сам бизнес операторов связи, делает целесообразным создание операторов виртуальных сетей, прилагающих дифференцированный сервис на строго определённую аудиторию пользователей, что дает новые маркетинговые преимущества.

Упомянутое разделение функций позволяет устранить определённые угрозы безопасности, но (нет ничего бесплатного в этом мире) создает и новые, что требует новых решений и новых средств.

Естественно возникает вопрос о том, почему в статье, посвященной SDN&NFV, мы заговорили про ICN? Дело в том, что SDN&NFV образуют очень удобную платформу для реализации DONA. SDN&NFV – это не конечная точка в развитии сетей, а лишь мостик к сетям нового поколения.

Это мостик позволяет реализовать DONA на уже хорошо протестированной и отработанной инфраструктуре современного Интернета.

Один из ключевых открытых вопросов переходного периода на поколение сетей ICN, это то, до какой степени он будет эволюционным?