

# Комплексное решение для оператора связи на базе архитектуры NFV

**А.А. РОЖКОВ, ведущий системный инженер ООО “Инлайн Телеком Солюшнс”,  
А.В. ПАВЛОВ, технический директор**

## Введение

Концепции Cloud, SDN, NFV широко известны. Не так давно и решения SD-WAN начали свое успешное развитие. Описания всех этих концепций можно найти в Сети, где они представлены подробно и на многих сайтах.

Каждая технология имеет свои слабые и сильные стороны, свои преимущества и ограничения. Cloud Computing, SDN, NFV и SD-WAN не исключения. В настоящей статье описывается один из вариантов применения решения для оператора связи, при котором эти концепции не конфликтуют, а дополняют и усиливают друг друга.

Для оператора связи, “погружающегося” в тему NFV, прежде всего,

необходимо четко понимать, какие именно сетевые функции возможно эффективно (во всех смыслах) виртуализировать. На сегодняшний день наиболее актуальными представляются сетевые функции защиты: VNF Firewall, VNF Web Application Firewall, VNF Email Security, VNF DDOS Protection.

Далее возникает вопрос обеспечения доступа к виртуальным сетевым функциям потребителей этих услуг. Ориентация только лишь на своих, уже имеющих клиентов операторских сервисов VPN, не дальновидна.

Следует использовать подходы OTT провайдеров услуг, предоставляющих свои сервисы вне зависимости от точки подключения клиен-

тов к Интернету. И решение здесь — SD-WAN.

Наработки в направлении облачных решений настолько успешны, что и выбор однозначен — “cattle not pets”, а реализация SDN в виде наложенной сети на базе виртуальных коммутаторов и туннелирования — следствие этого выбора.

Итак, общая картина вполне логична и понятна. Но детали требуют проработки. Практически все производители заявляют о полном соответствии своих продуктов общепринятым открытым стандартам (например, NFV-MANO Framework в версии ETSI), но собственно frameworks оставляют многие вопросы реализации тех или иных функций на откуп производителям. Поэтому наи-

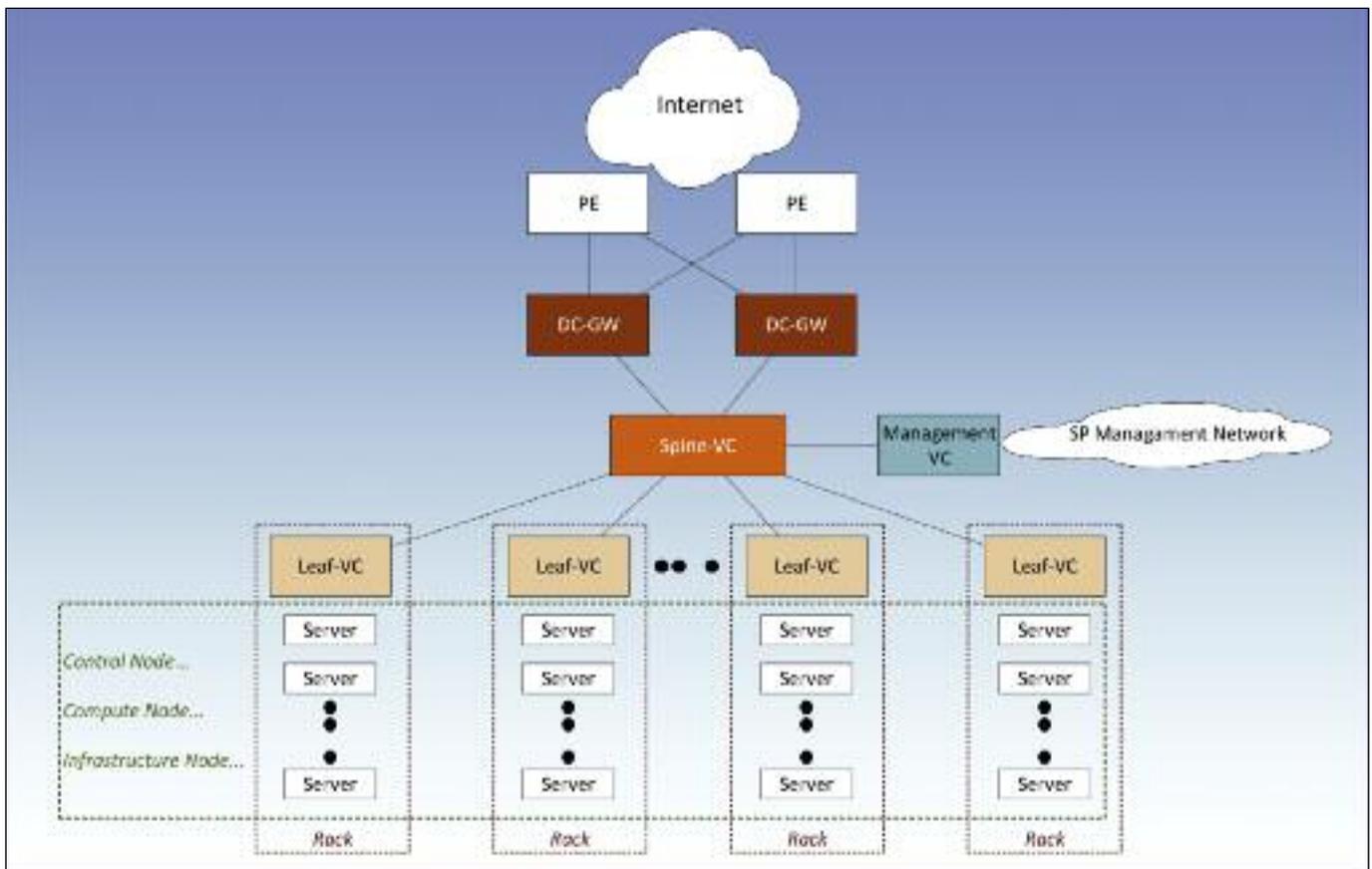


Рис. 1. Сетевая топология Virtual Chassis

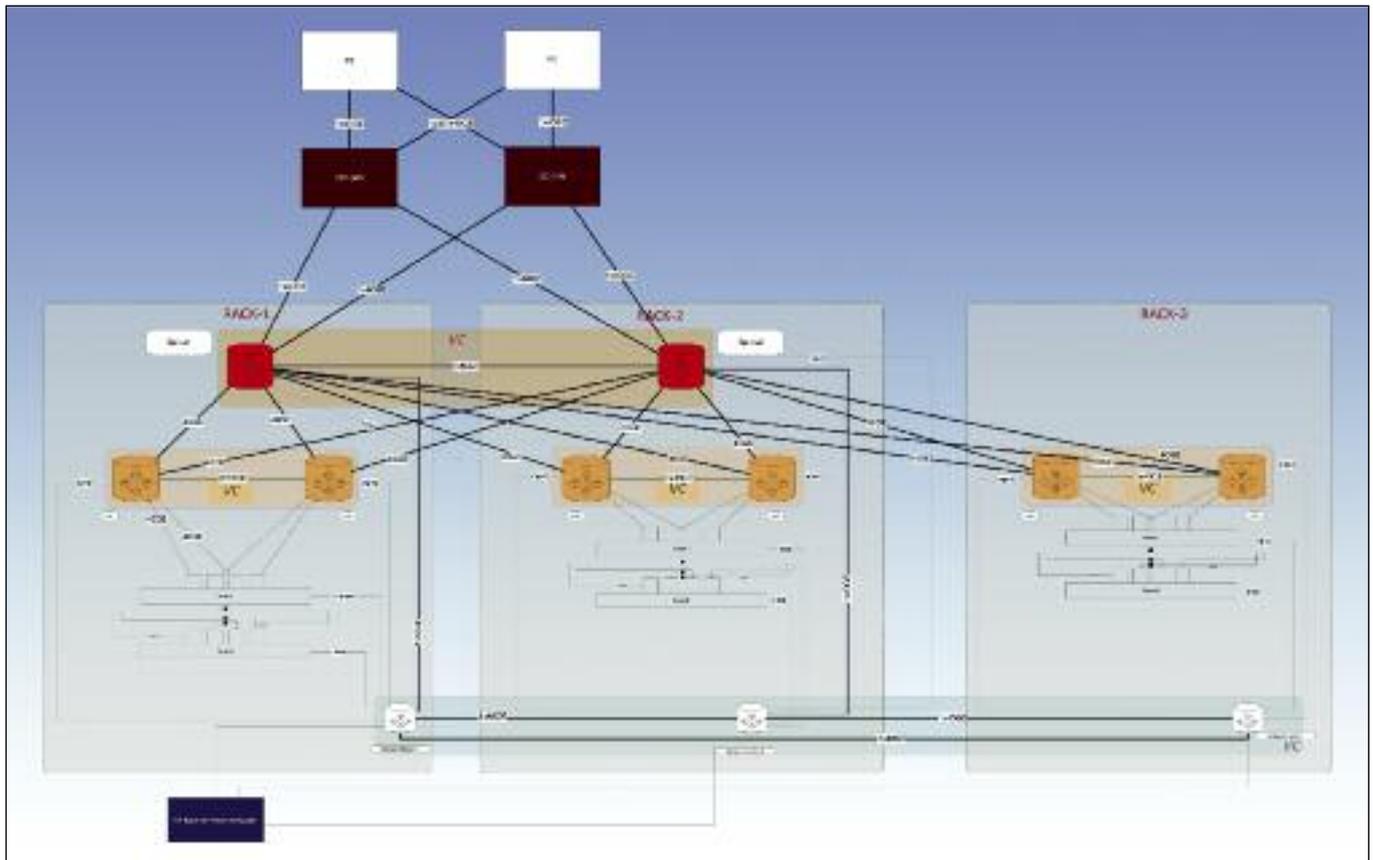


Рис. 2. Сетевая топология соединения spine-leaf

менее проблемным решением является то, при котором вся наложенная сетевая инфраструктура (продукты SD-WAN, SDN и Data Center Gateway) представлена одним и тем же производителем.

### Инфраструктура

Инфраструктурные элементы решения — DC-GW, сетевые коммутаторы, образующие spine-leaf фабрику, серверы.

DC-GW подключен, с одной стороны, к PE маршрутизаторам оператора, которые обеспечивают каналы в Интернет, а также доступ к различным VPN-сервисам оператора (в частности EVPN), с другой — к spine-leaf фабрике, которая обеспечивает связность серверов и DC-GW.

Серверы используются для размещения:

- управляющих компонентов NFV MANO — NFV-O, VNFM, VIM (Control Nodes облачного решения Open-Stack);

- компонентов NFVI — Compute Nodes в облачном решении Open-Stack;

компонентов SD-WAN решения (пограничный VXLAN шлюз между DC доменом и WAN доменом);

компонентов вспомогательных инфраструктурных сервисов (RA-VPN, Firewall, DNS, SSL-Proxy, Load Balancer).

Spine-leaf фабрика в данном решении обеспечивает L2 связность серверов между собой и доступность DC-GW. Два leaf коммутатора, а также spine коммутаторы в стойке объединены в одно виртуальное шасси. Leaf VC подключаются к spine VC с помощью обычного LAG. В каждой стойке присутствует коммутатор для внешнего управления, все OOBM также объединены в одно виртуальное шасси.

Отдельное VC коммутаторов OOB управления инфраструктурой подключено к spine VC обычным LAG. Таким образом на уровне VC вся spine-leaf фабрика представляет простейшую топологию “звезда” (рис. 1).

При том, что на физическом уровне все соединения между leaf и spine коммутаторами выполнены именно по классической spine-leaf

схеме, DC-GW также подключены к spine VC обычным LAG (рис. 2).

Применение виртуального шасси обеспечивает достаточный уровень масштабирования L2 фабрики без использования каких-либо механизмов исключения петель или Underlay SDN для инфраструктуры фабрики.

Добавление новой стойки с leaf VC на уровне Control Plane означает только лишь дополнительный луч к spine VC, при том, что на уровне Data Plane каждый из двух leaf коммутаторов новой стойки подключается к каждому spine коммутатору двумя физическими соединениями.

Добавление нового spine switch означает лишь увеличение количества портов в spine VC. Таким образом, L2 фабрика служит стабильным основанием для динамичных соединений наложенной сети между VTEP серверов и VTEP DC-GW. Количество VTEP не велико, и технология виртуального шасси с единой FIB для всех участников в данном случае не является ограничением. Underlay SDN для такой spine-leaf фабрики — совсем не нужное обременение.

Все соединения L2 фабрики — 40GE. И серверы также подключены к фабрике 40GE интерфейсами. Не соответствие пропускной способности суммарной полосы портов доступа и суммарной полосы связей spine-leaf объясняется тем, что четыре 40GE порта сетевой карты сервера, конечно, никогда не будут заполнены. 40 GE порты были выбраны потому, что 40GE интерфейс обеспечивает существенно меньшую задержку, чем 10GE интерфейс.

В связи с тем, что трафик клиентов проходит через цепочку различных VNF, расположенных возможно на разных физических серверах, то задержка на каждом сервере должна быть минимальной, и 40GE интерфейсы помогают в этом.

Осталось добавить, что CPE, используемое в SD-WAN части решения, — достаточно простое устройство, FIB таблицу которого заполняет SD-WAN SDN контроллер. SD-WAN решение обеспечивает двухфакторную авторизацию CPE устройства в системе SD-WAN (e-mail и контрольный код через

SMS) и не требует высокой квалификации сотрудника, выполняющего его установку и регистрацию CPE.

### NFV MANO

В комплексном решении NFV для оператора связи End-to-End сервис состоит из множества отдельных, но требующих сопряжения услуг сети, развертываемых, как минимум, в подсистемах SD-WAN и DC. Задачи резервирования, в том числе и георезервирования, на базе VNF также усложняют структуру E2E сервиса. Тем не менее, только составная модель E2E сервиса может обеспечить необходимую гибкость решения, широкие возможности его развития в дальнейшем и модификацию под новые требования.

В стандартах ETSI пока что однозначно не определены зоны ответственности для NFVO и для OSS с точки зрения End-to-End сервиса. В конечном итоге это задается возможностями как NFVO, так и OSS.

В данном случае быстрый и простой NFVO работает на уровне

отдельных услуг сети. Композицию же E2E сервиса, включая запуск всех его составляющих, осуществляет OSS, контролируя их согласованность и порядок запуска при обращении к NFVO. OSS получает/запрашивает разнообразные параметры из различных систем оператора связи, в том числе из BSS, определяющие E2E сервис для данного клиента. На основе этих параметров OSS формирует свой список значений для заполнения параметров всех NSD, из которых и “склеивается” E2E сервис (конечно, OSS хранит все NSD ID и NSR ID, входящие в E2E). Выполняя запросы к NFVO, OSS последовательно запускает эти NSD, в результате выстраивая E2E сервис.

Таковы ключевые особенности данного комплексного решения на базе архитектуры NFV для операторов связи.



**105082, Москва, ул. Большая Почтовая,  
д. 26 В, стр. 2  
info@ininetecom.ru**