ЦЕНТР ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ КОМПЬЮТЕРНЫХ СЕТЕЙ

ETHERNET FORUM

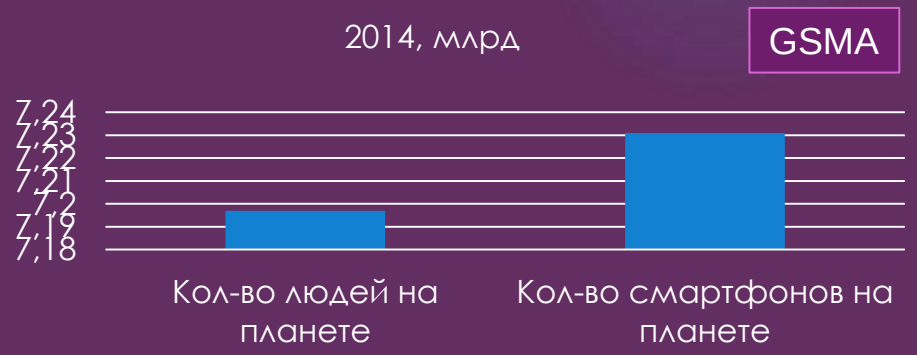
SDN & NFV: новые горизонты

Руслан Смелянский
директор ЦПИКС, профессор МГУ им. Ломоносова, д.ф-м.н, член-корреспондент РАН

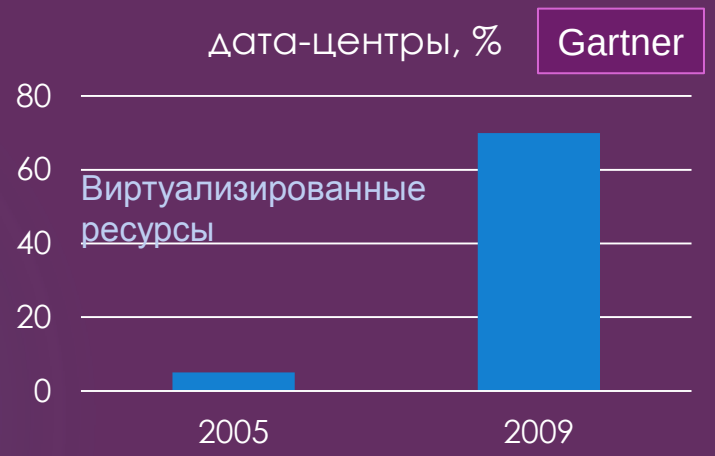
Москва, октябрь 2015

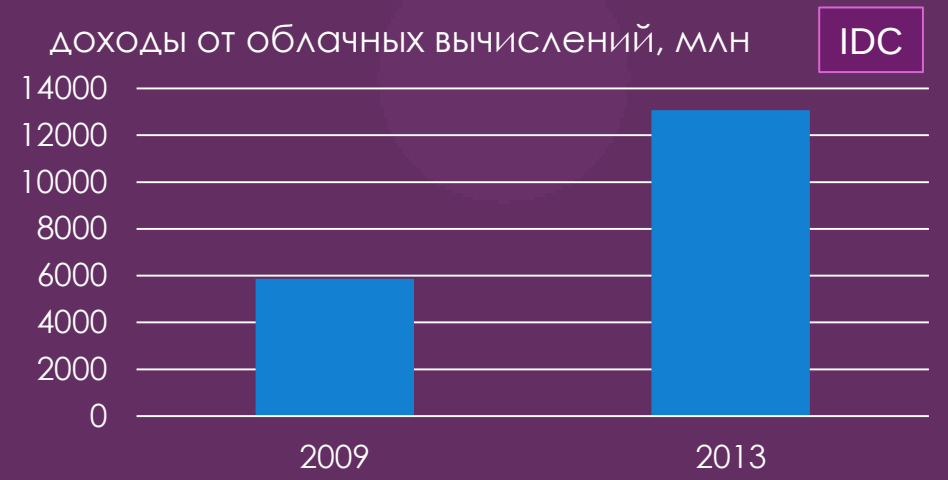
Тенденции развития рынка информационных технологий

Мобильность



Виртуализация

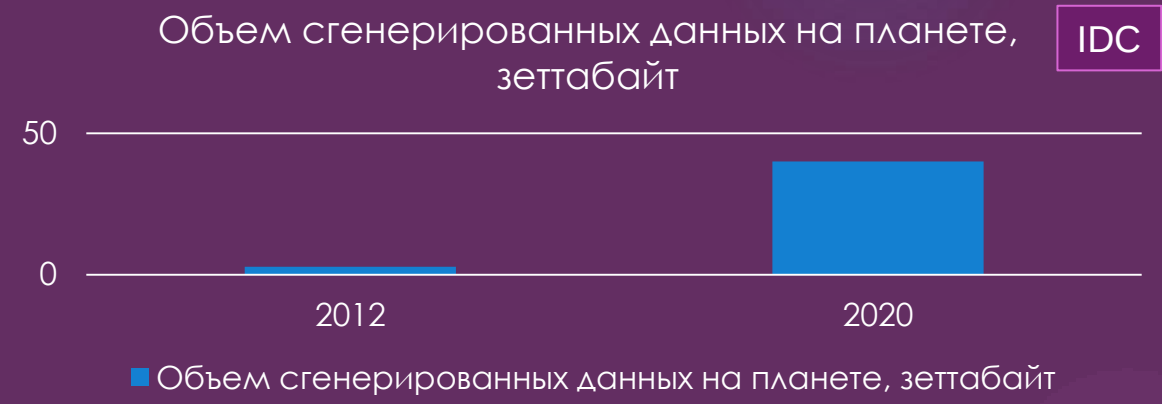




Консолидация инфраструктуры

Тенденции развития рынка информационных технологий

Big Data



Всего с начала 2010 г. объем хранимых данных вырос в 50 раз

Центры обработки данных

- В 2014 году объем мирового рынка колокации в ЦОДах составил $22,8 млрд. Общая площадь размещения оборудования достигла 10,13 кв. км. (451 Research)
- Общее число дата-центров всех типов в 2017 г. вырастет до 8,6 млн (IDC)

Телеком

- Каждый из пользователей глобальной сети генерирует больше трафика, чем вся Всемирная паутина 30 лет назад
- В 2014 году интернет-трафик вырос, по сравнению с 1984 годом, в 2,7 миллиардов раз (Cisco)

Изменение бизнес-модели

РЕНТАБЕЛЬНОСТЬ БИЗНЕСА

Промышленное производство

Энергодобыча

Тяжелая и легкая промышленность

РЕНТАБЕЛЬНОСТЬ БИЗНЕСА

Оператор связи

Интернет провайдер

Доступ к «транспорту» должен быть бесплатным, платным должен стать контент и услуги.

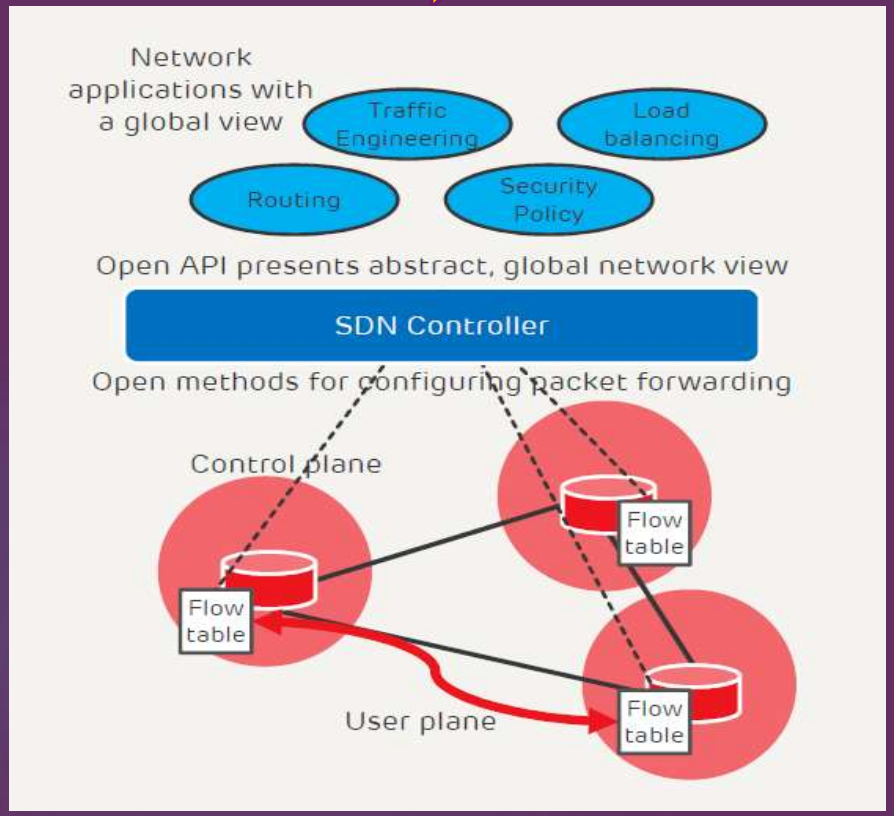
Информация о пользователе:

- Использование: посещаемые сайты, звонки и сообщения (включая тип сообщений и их частоту);
- География: где находится мобильное устройство в конкретный момент (уровень точности может разниться от района к району);
- Демография: доход домохозяйства, число и возраст проживающих детей;
- Уровень дохода: тарифный план, история платежей, паттерн совершения покупок;
- Мультиплатформенность: использование данных на разных устройствах и типах подключения к сети (3G, WiFi и т.п.).

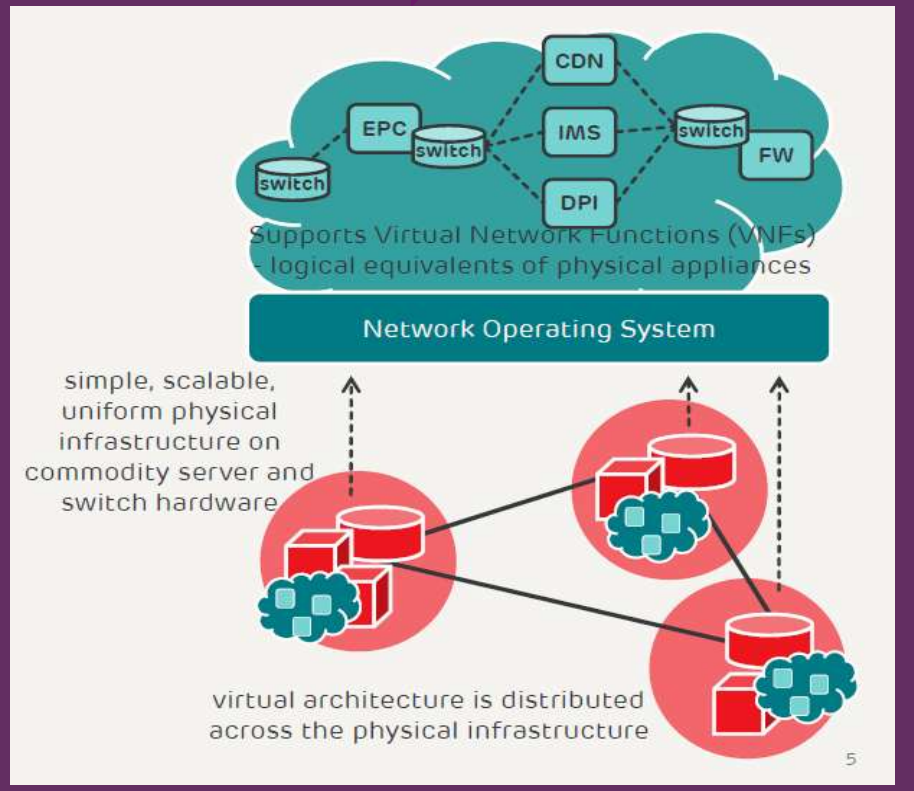
- 2011 - AT&T – запуск подразделения AdWorkds: поддержка целевой рекламы в web, мобильной среде и ТВ.
  2013 – AdWorks открывает доступ к анализу данных 70 млн. пользователей.
- 2012 – Verizon - запуск инициативы Precision Market Insights – доступ к мобильным данным пользователей для маркетинговых и рекламных компаний.

SDN и NFV : схожести и различия

ИТ **с 2007 года** SDN



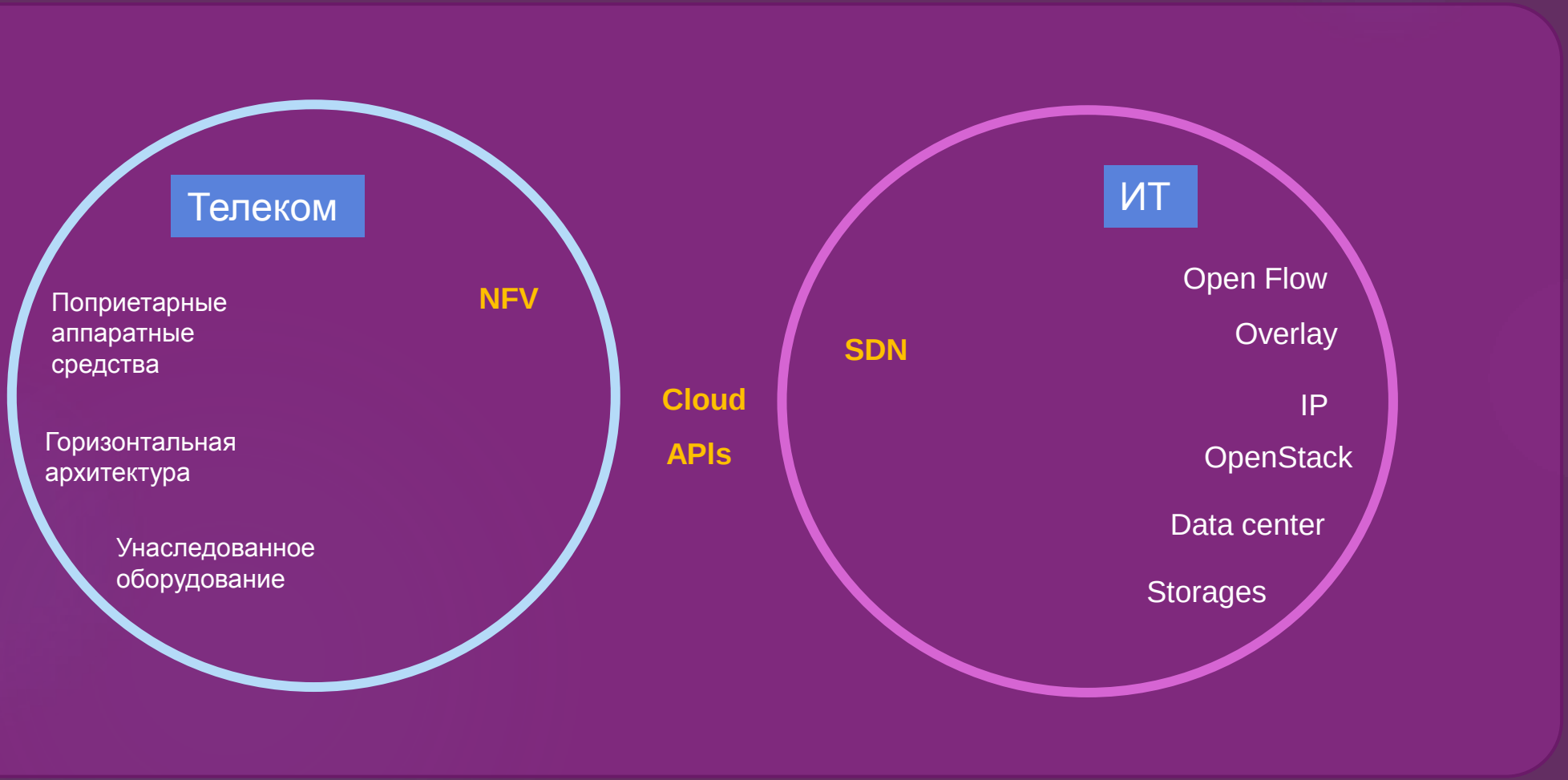
Телеком **с 2012 года** NFV



IBM, HUAWEI, NEC, BROCADE, hp, CISCO, big switch networks, JUNIPER NETWORKS, Extreme networks Ethernet Everywhere

NTT, at&t, Telefonica, Deutsche Telekom, CONTEXTREAM, sandvine Intelligent Broadband Networks, Alcatel-Lucent communications, Sonus NETWORKS, Metaswitch Networks, nuagenetworks

Симбиоз SDN и NFV



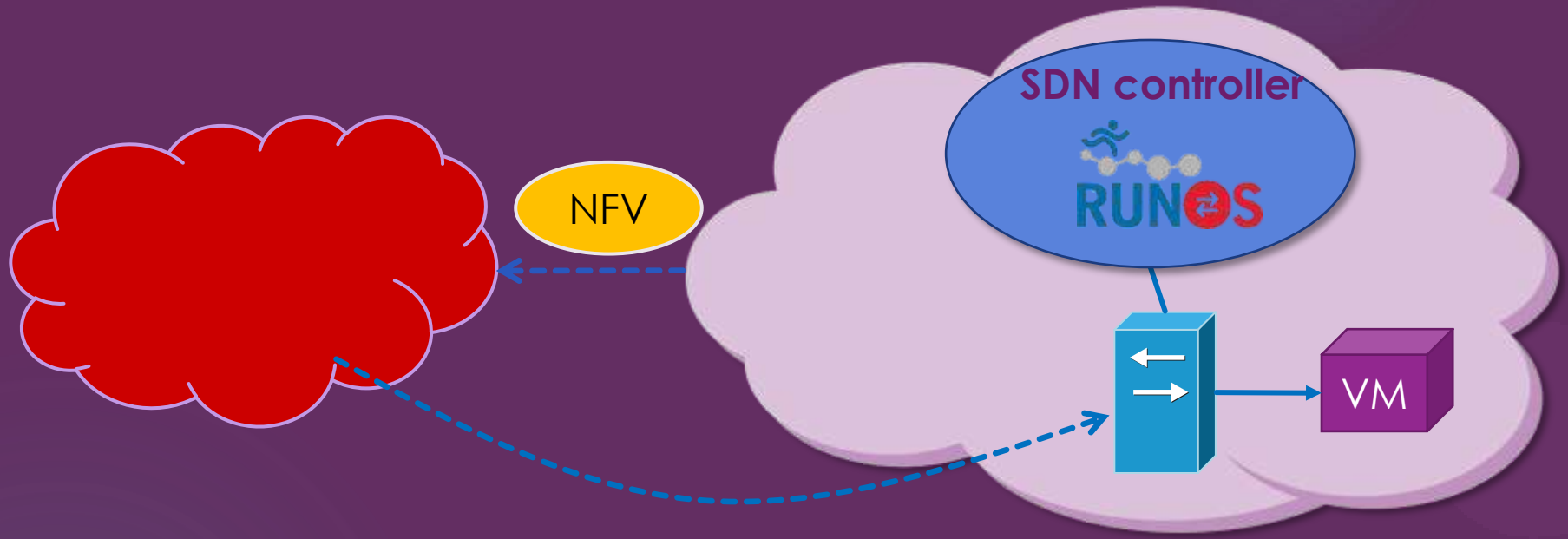
1 NFV / SDN

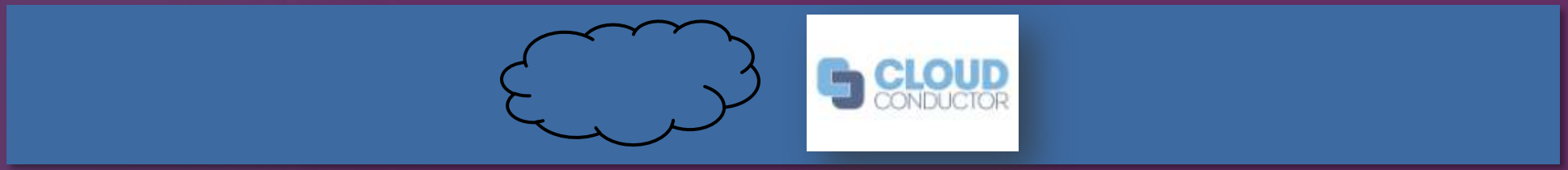
2 SDN / NFV

3 SDN NFV

Пример 1 сценария

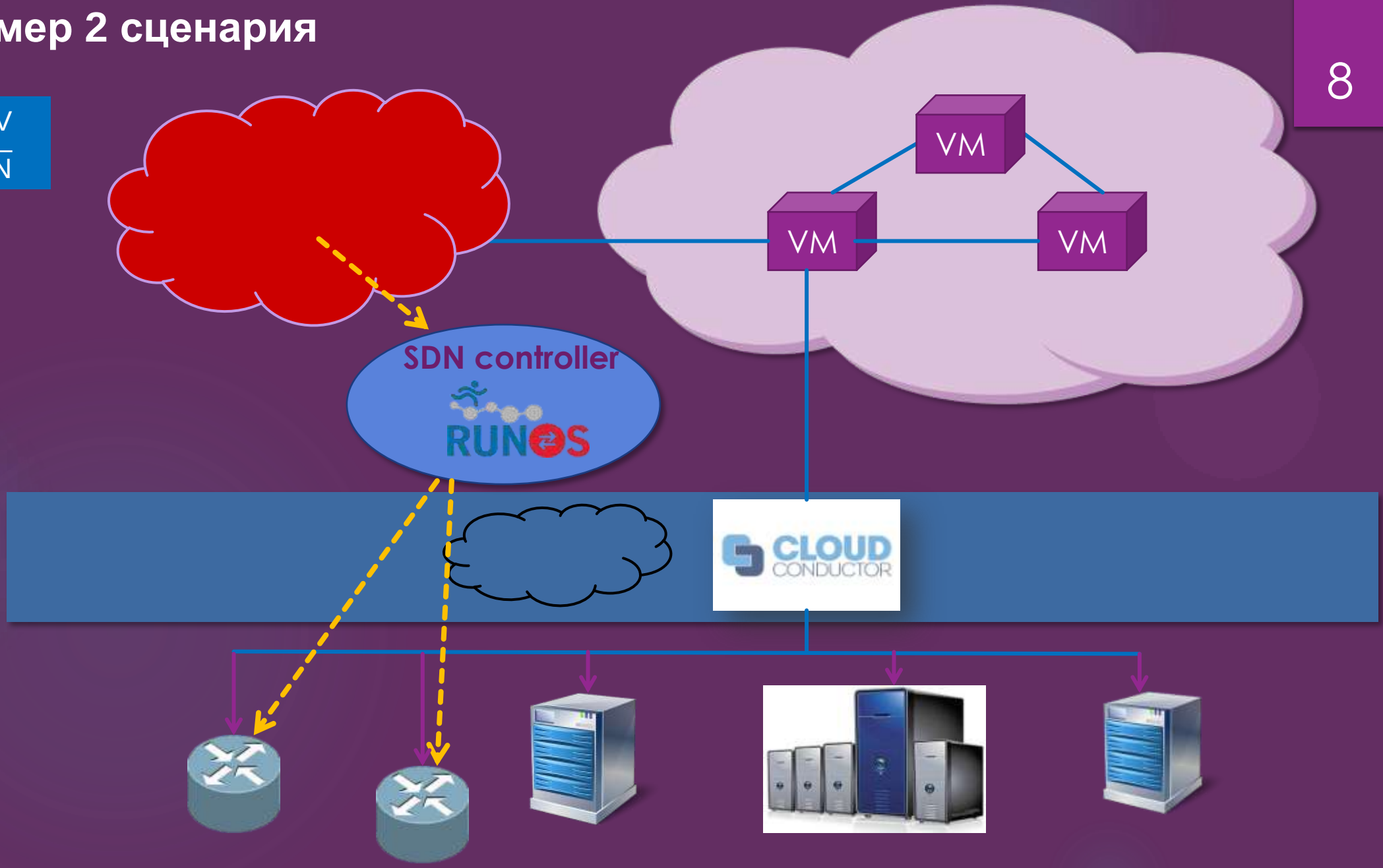
SDN
NFV



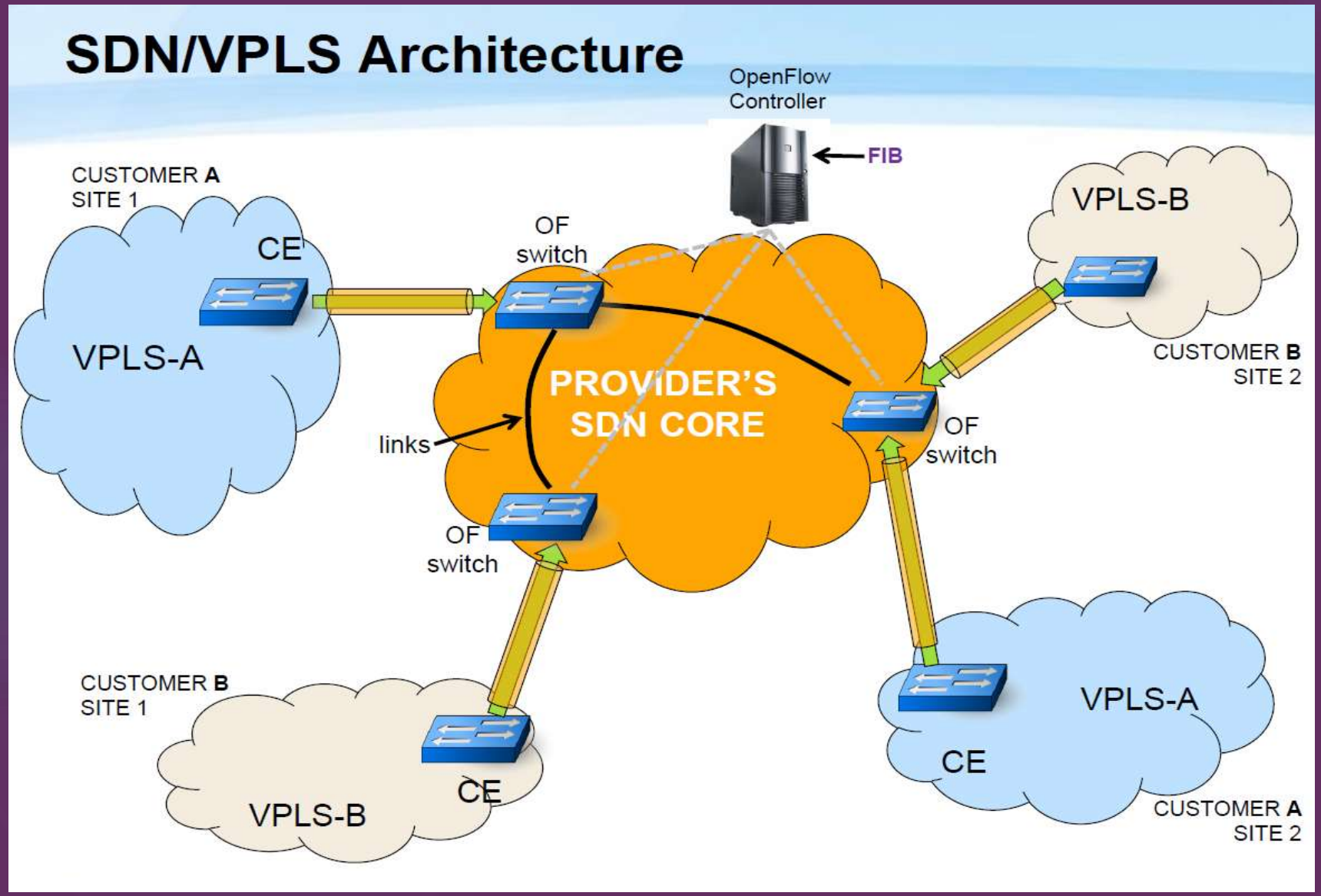


Пример 2 сценария

NFV
SDN



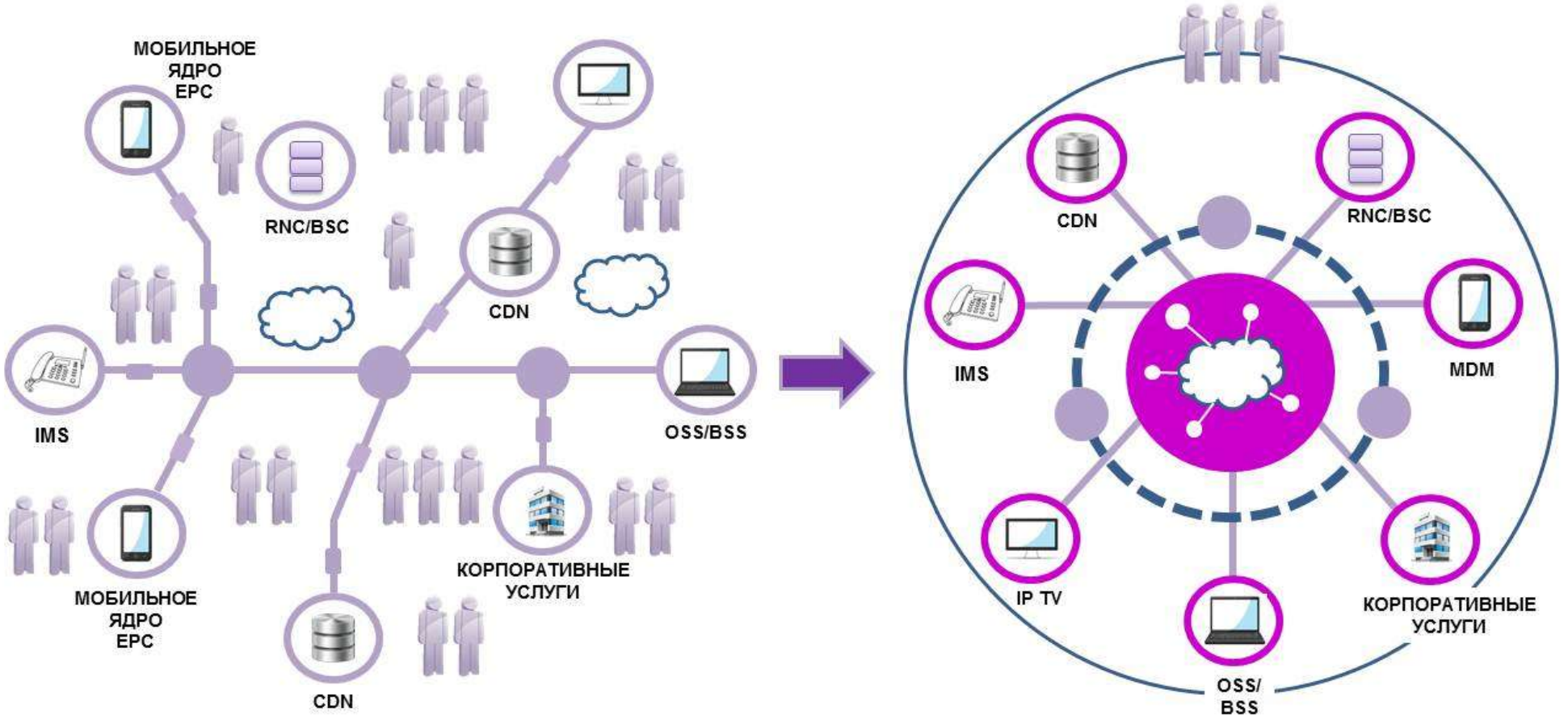
SDN & VPN



Источник: S.Konstantares, G.Thesolonikets Software Defined VPNs. University of Amsterdam, 2014

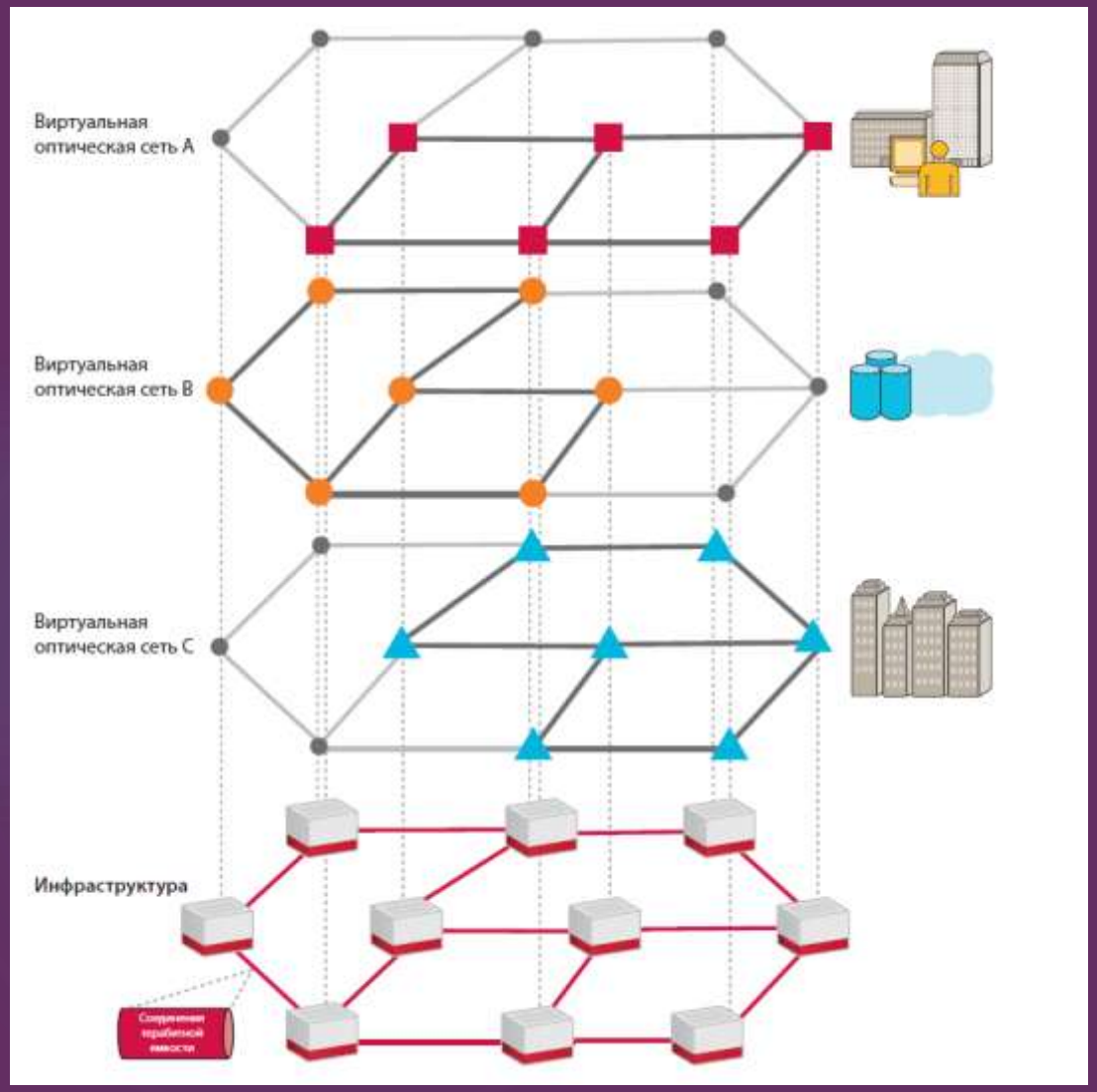
Пример 3 сценария

SDN и NFV

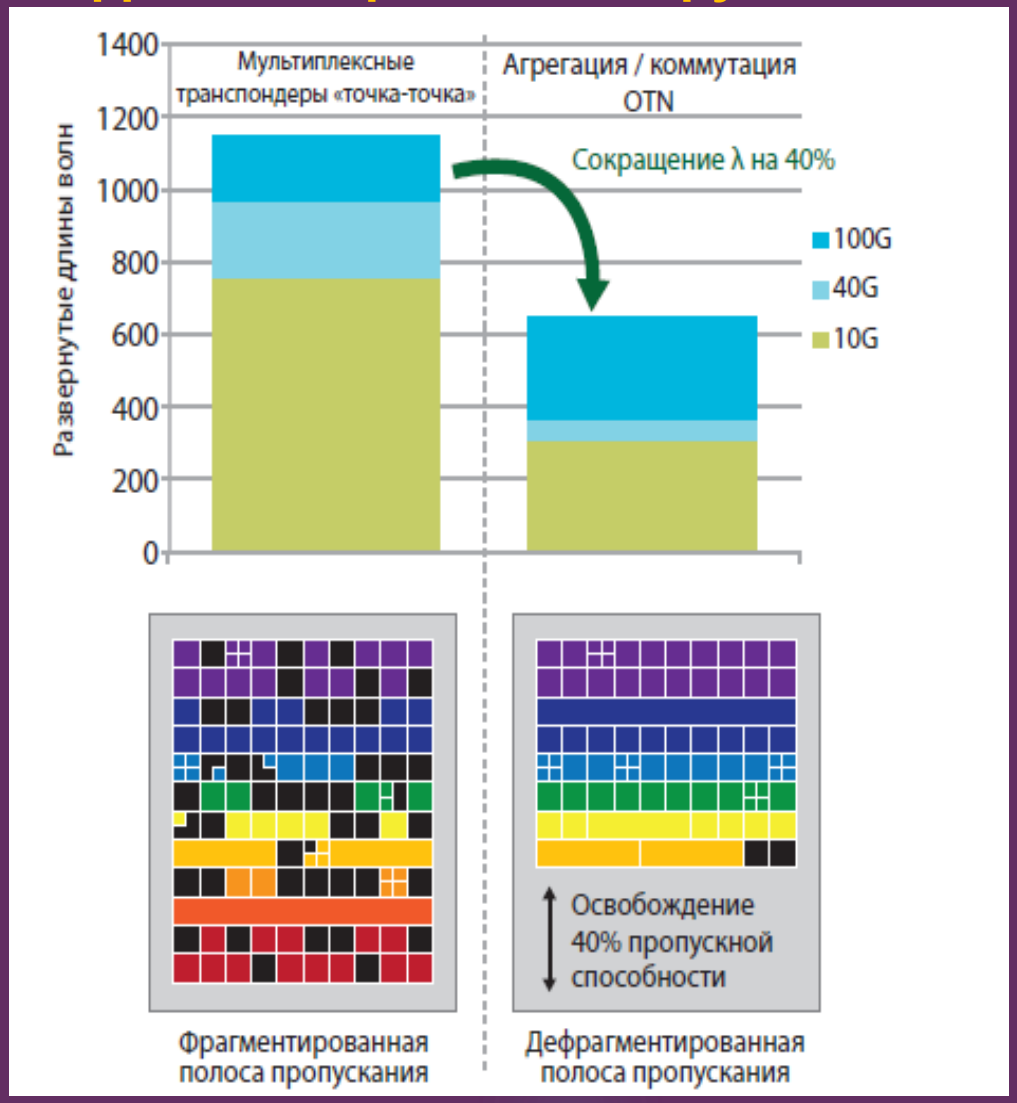


Optical Transport Networks

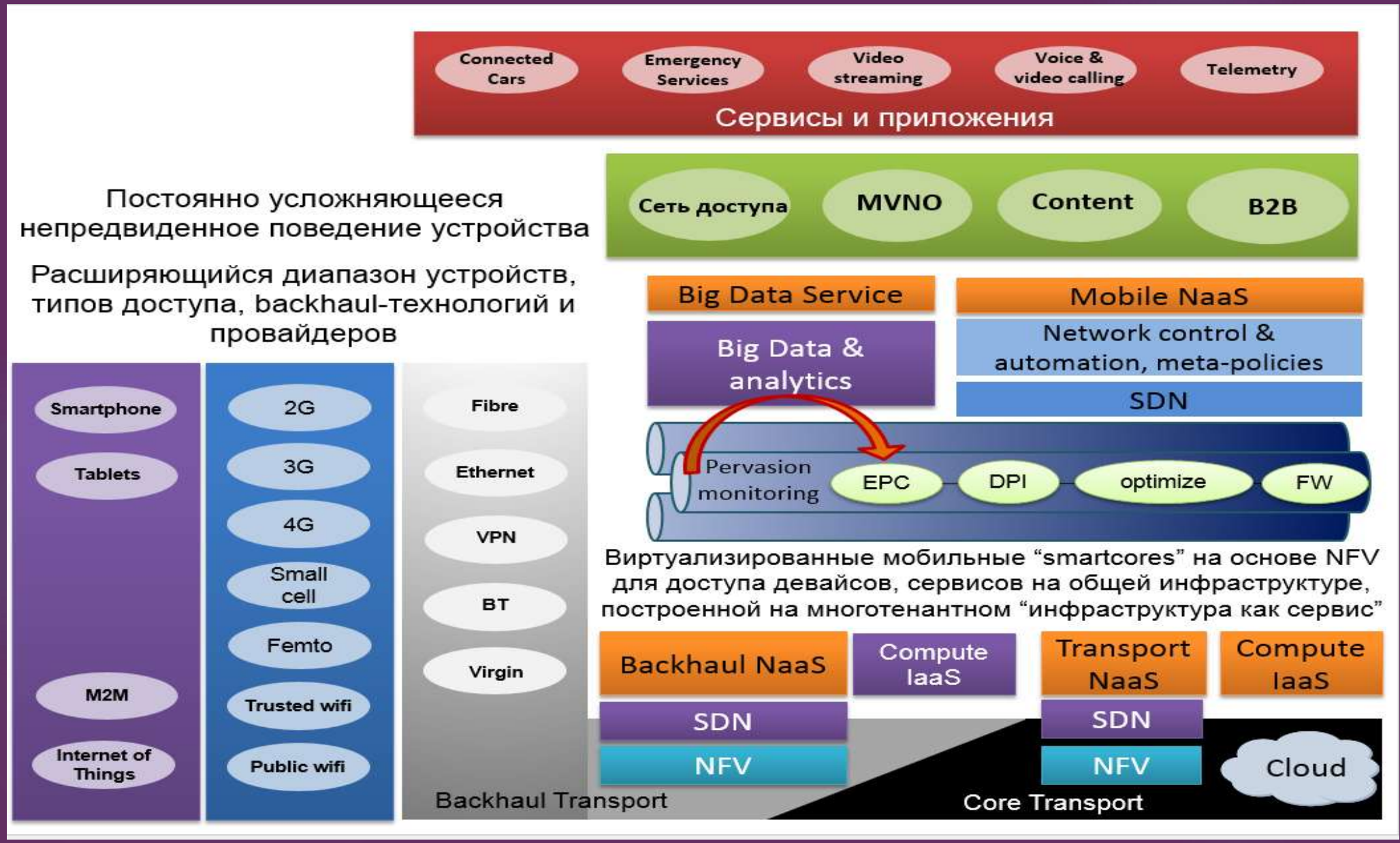
Виртуальные сети на база OTN



Дефрагментирование загрузки линий



Use-Case: Mobile SDN



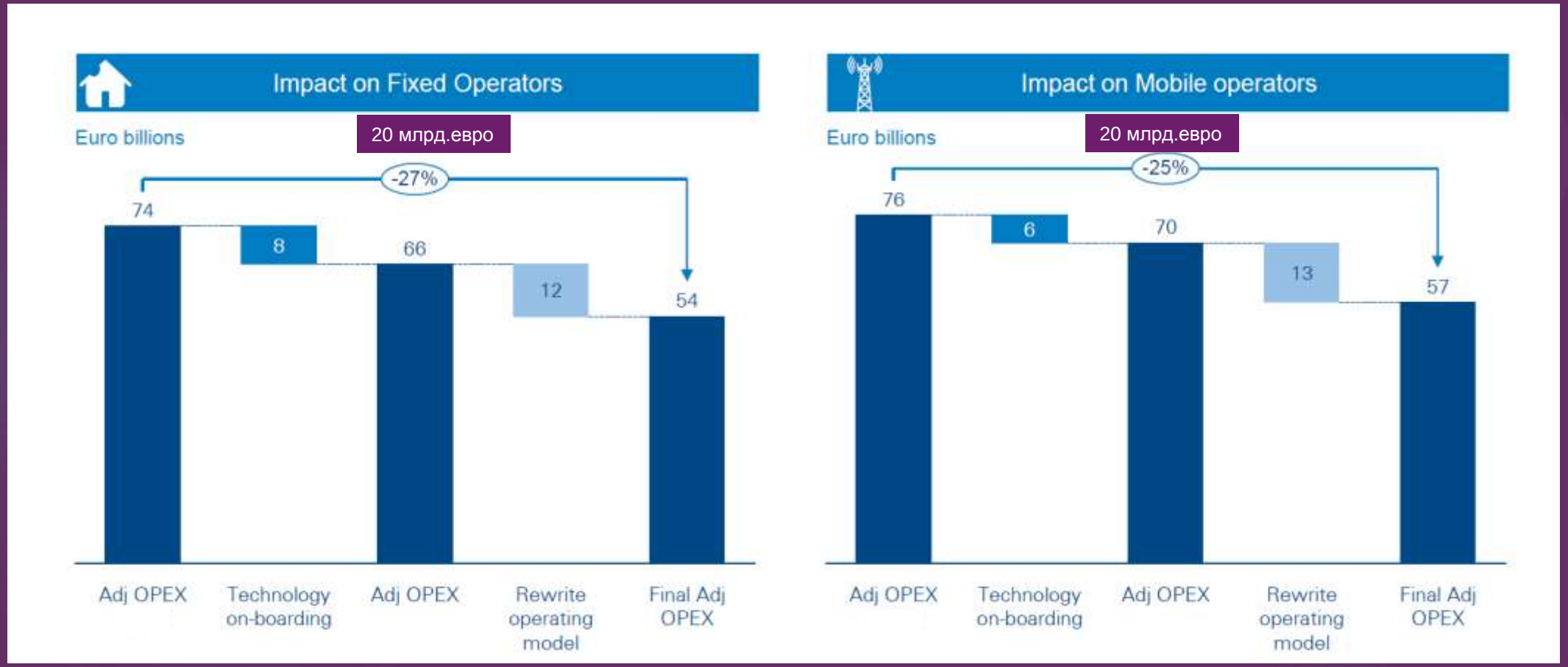
Источник: Revolutionisingmobile networks with SDN and NFV / Cambridge Wireless Virtual Networks SIG, Philip Bridge, Senior Network Architect at EE, 2014

Use-case: Transport – SDN

Источник: Telefonaktiebolaget LM Ericsson 2015 | MPLS SDN World Congress & NFV/SDN Summit 2015, Paris

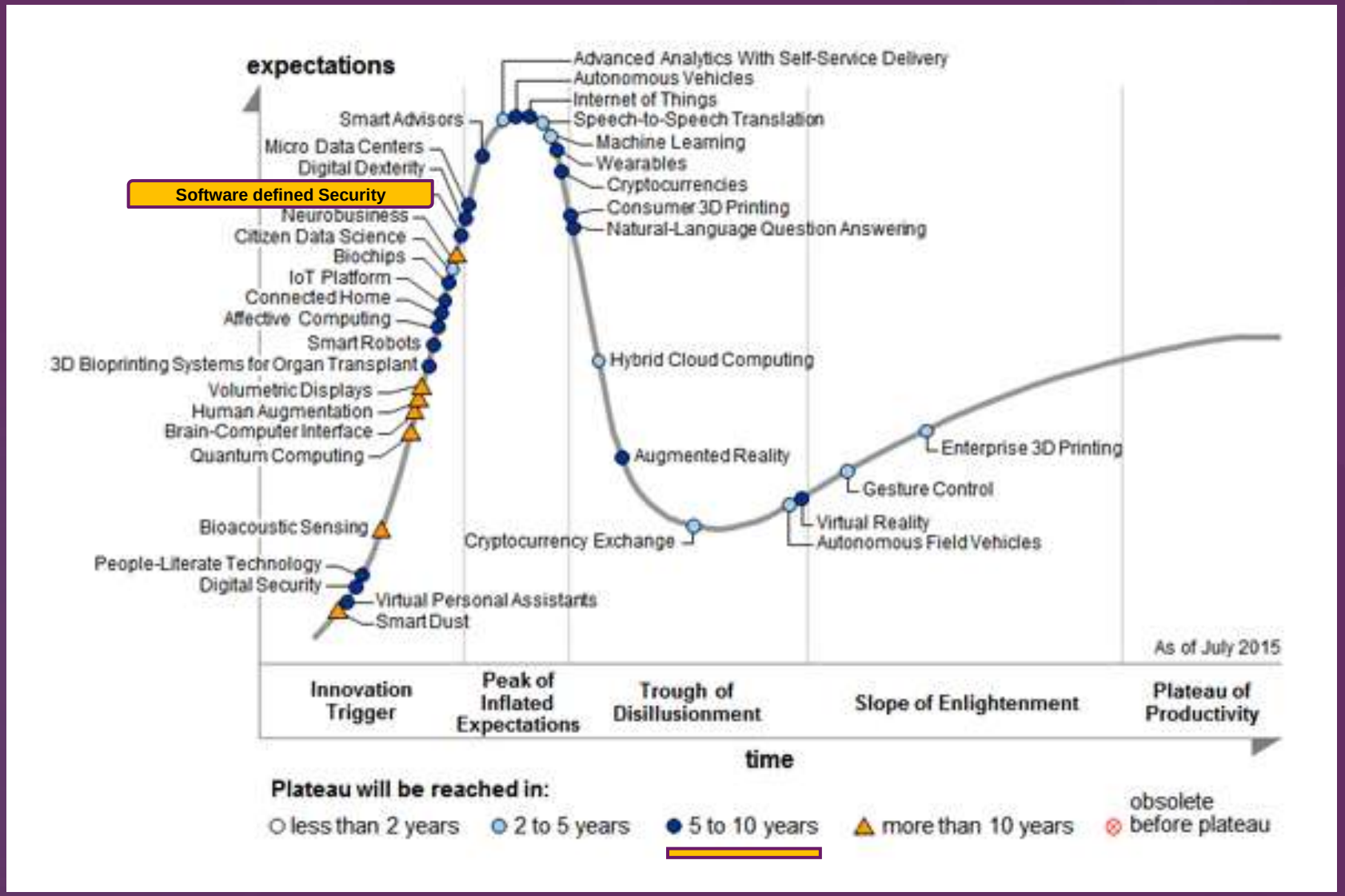
Оценка эксплуатационных затрат в фиксированной и мобильной связи с использованием SDN и NFV

Опрос проводился среди 35 европейский операторов.
Коллективный доход которых в 2013 году составил 250 млрд.евро, годовой OPEX составил 150 млрд.евро.
Общее количество сотрудников – 665 000 человек.



Источник: Bell Labs/Alcatel Lucent «Reshaping the future with NFV and SDN», 2015

Use-Case: SDN - безопасность



Источник: Gartner (2015)

SDN - безопасность


```
-------------------------------------------------
 LINK INFO FROM DB : Count = 1
-------------------------------------------------
 LINK_TABLE_NAME      = controller_link
 LINK_ID              = 00:00:00:00:00:00:00:01-2-00:00:00:00:00:00:00:02-2
 LINK_SRC_SWITCH      = 00:00:00:00:00:00:00:01
 LINK_SRC_PORT        = 2
 LINK_SRC_PORT_STATE  = 0
 LINK_DST_SWITCH      = 00:00:00:00:00:00:00:02
 LINK_DST_PORT        = 2
 LINK_DST_PORT_STATE  = 0
 LINK_VALID_TIME      = 1390964347029
 LINK_TYPE            = internal
-------------------------------------------------
```

Link 1

```
-------------------------------------------------
 LINK INFO FROM DB : Count = 2
-------------------------------------------------
 LINK_TABLE_NAME      = controller_link
 LINK_ID              = 00:00:00:00:00:00:00:02-2-00:00:00:00:00:00:00:01-2
 LINK_SRC_SWITCH      = 00:00:00:00:00:00:00:02
 LINK_SRC_PORT        = 2
 LINK_SRC_PORT_STATE  = 0
 LINK_DST_SWITCH      = 00:00:00:00:00:00:00:01
 LINK_DST_PORT        = 2
 LINK_DST_PORT_STATE  = 0
 LINK_VALID_TIME      = 1390964347026
 LINK_TYPE            = internal
-------------------------------------------------
```

Link 2

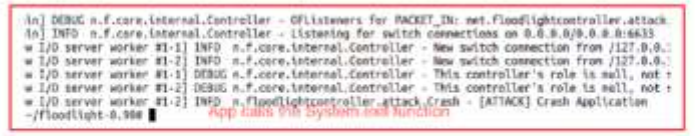
```
yw - [ATTACK]-------------------------------------------------
yw - [ATTACK] LINK INFO FROM DB : Count = 1
yw - [ATTACK]-------------------------------------------------
yw - [ATTACK] LINK_TABLE_NAME      = controller_link
yw - [ATTACK] LINK_ID              = 00:00:00:00:00:00:00:02-2-00:00:00:00:00:00:00:01-2
yw - [ATTACK] LINK_SRC_SWITCH      = 00:00:00:00:00:00:00:02
yw - [ATTACK] LINK_SRC_PORT        = 2
yw - [ATTACK] LINK_SRC_PORT_STATE  = 0
yw - [ATTACK] LINK_DST_SWITCH      = 00:00:00:00:00:00:00:01
yw - [ATTACK] LINK_DST_PORT        = 2
yw - [ATTACK] LINK_DST_PORT_STATE  = 0
yw - [ATTACK] LINK_VALID_TIME      = 1390964347826
yw - [ATTACK] LINK_TYPE            = internal
yw - [ATTACK]-------------------------------------------------
yw -
 [ATTACK] Access InternalDB : delete Link Information
```

Link 2 Only
Link 1 has been deleted

```
2014-05-12 09:26:33.219 PDT [Statistics Collector] DEBUG o.o.c.p.o.i.InventoryServiceShim - Connection service
accepted the inventory notification for OF|00:00:00:00:00:00:00:02 CHANGED
2014-05-12 09:26:34.217 PDT [Statistics Collector] DEBUG o.o.c.c.internal.ConnectionManager - updateNode: OF|00
:00:00:00:00:00:00:03 type CHANGED props [Description[None]]
2014-05-12 09:26:34.217 PDT [Statistics Collector] DEBUG o.o.c.s.internal.SwitchManager - updateNode: OF|00:00:
00:00:00:00:00:03 type CHANGED props [Description[None]] for container default
2014-05-12 09:26:34.217 PDT [Statistics Collector] DEBUG o.o.c.p.o.i.InventoryServiceShim - Connection service
accepted the inventory notification for OF|00:00:00:00:00:00:00:03 CHANGED
2014-05-12 09:26:51.791 PDT [SwitchEvent Thread] DEBUG o.o.c.h.internal.HostTracker - Received for Host: IP 10.
0.0.1, MAC 000000000001, HostNodeConnector [nodeConnector=OF|1@OF|00:00:00:00:00:00:00:01, vlan=0, staticHost=f
alse, arpSendCountDown=0]
2014-05-12 09:26:51.794 PDT [Thread-37] DEBUG o.o.c.h.internal.HostTracker - New Host Learned: MAC: 00000000000
1  IP: 10.0.0.1
2014-05-12 09:26:51.794 PDT [Thread-37] DEBUG o.o.c.h.internal.HostTracker - Notifying Applications for Host 10
.0.0.1 Being Added
2014-05-12 09:26:51.795 PDT [Thread-37] DEBUG o.o.c.h.internal.HostTracker - Notifying Topology Manager for Hos
t 10.0.0.1 Being Added
2014-05-12 09:26:51.796 PDT [SwitchEvent Thread] INFO  o.o.controller.attack.crash.Crash - [ATTACK.CRASH] Packe
t Received
2014-05-12 09:26:51.796 PDT [SwitchEvent Thread] INFO  o.o.controller.attack.crash.Crash - [ATTACK.CRASH] Syste
m.exit() called
2014-05-12 09:26:51.798 PDT [Listener:59957] DEBUG com.arjuna.ats.arjuna - Recovery listener existing com.arjun
a.ats.arjuna.recovery.ActionStatusService
2014-05-12 09:26:51.798 PDT [Thread-11] DEBUG org.jgroups.stack.GossipRouter - ConnectionHandler[peer: /127.0.0
.1, logical_addrs: localhost-12306] is being closed
2014-05-12 09:26:51.805 PDT [Thread-11] DEBUG org.jgroups.stack.GossipRouter - router stopped
$
```

Call a System Exit Function

OpenDayLight has been crashed



App calls the System.exit function

Flood Light - Out of Memory Error

```
def handle_PacketIn(event):
    packet = event.parsed
    inport = event.port
    .....
def launch():
  core.openflow.addListenerByName("PacketIn", handle_PacketIn)
  print '[ATTACK] Crash Application'
  sys.exit(0)
```

App calls the System.exit function

```
openflow@openflowtutorial:~/pox$ ./pox.py monitoring crash
POX 0.0.0 / Copyright 2011 James McCauley
[ATTACK] Crash Application
openflow@openflowtutorial:~/pox$ _
```

Crash App Kills monitoring App and POX

Java Out of Memory Error

Источник: KAIST Atto Research Korea, 2014

SDN - безопасность

Устройства OF сети – Data Plane

- Уязвимости программного обеспечения
  a. неустойчивость кода к внешним воздействиям
  b. код с уязвимостями
- Атаки с использованием вредоносного кода
- DDoS атаки
- Атака сетевых устройств изнутри сети
- Вредоносные устройства в OF-сети

Контроллер

- Обеспечение безопасности контроллера
- Компрометация контроллера позволяет атакующим управлять всей сетью
- DDoS атаки на контроллер
- Поддельный контроллер может изменять топологию сети
- Строгий механизм аутентификации для доступа к SDN-контроллеру
- Целостность контроллера
- Внедрение нежелательной информации в контроллер

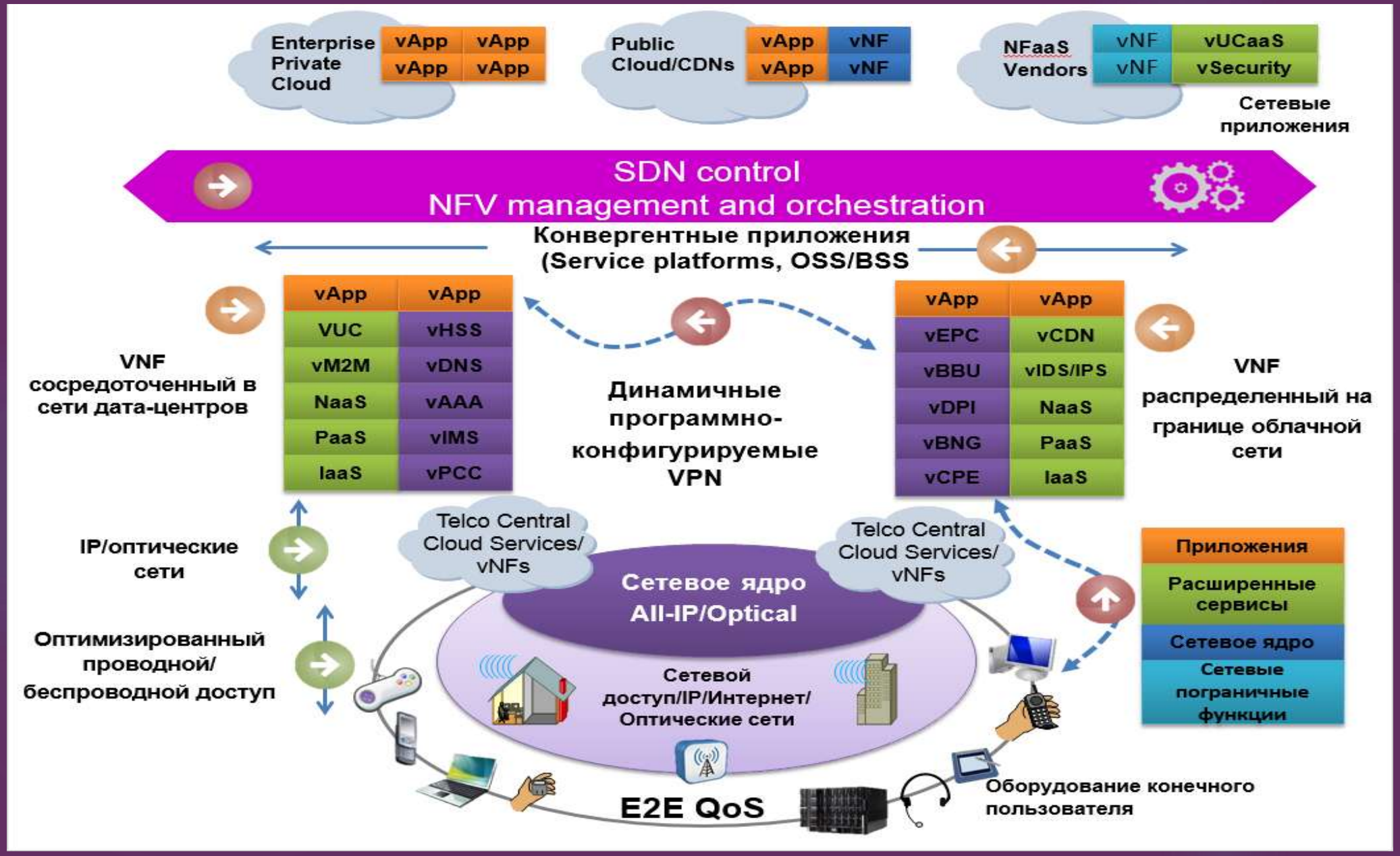
Каналы связи

- В каналах Open Flow используются SSL/TLS, но данные протоколы не являются обязательными
- Аутентификация между контроллером и OF устройствами
- DDoS атаки – поддержание насыщенности канала

Control Plane

- Требуется обеспечение безопасности control plane, управление авторизацией доступа для сетевых приложений
- Требуется аутентификация доступа приложений на control plane
- Сеть должна обслуживать требования бизнес приложений, и логика данный приложений определяет способы обеспечения безопасности

Конвергентная сеть



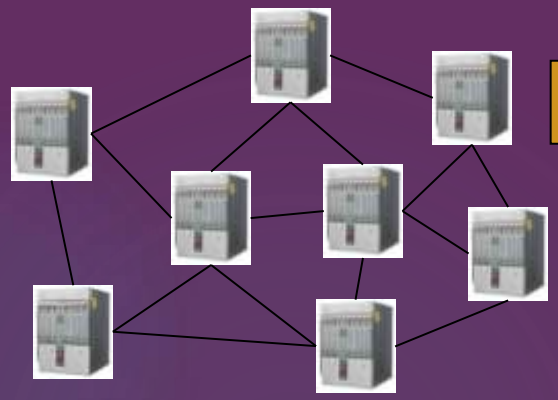
Источник: Bell Labs Alcatel Lucent «Reshaping the future with NFV and SDN», 2015

Информационная сеть vs Компьютерная сеть

Information Centric Networking

Интернет сегодня

Акцент на *узлах*



В современном интернете доминирующая функция – доступ к информации!

Evolution

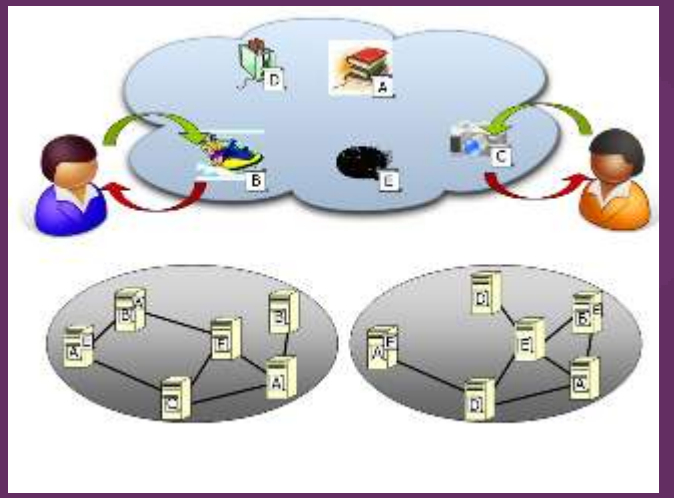
Web

CDN

P2P

Information Centric Network

Фокус на объектах информации



Важные требования:

- доступ к названным ресурсам, а не хостам
- масштабируемое распределение через репликацию и кэширование
- хороший контроль разрешающей способности маршрутизации и доступа

С повсеместным кэшированием, НО для всех приложений и для всех пользователей и провайдеров контента!

Потенциальные новые ниши для SDN и NFV

Динамическое обеспечение услуг

- Предоставление пропускной способности по требованию
- Расширение возможности управления пользователем виртуальными сетями (тенант)
- Эластичная пропускная способность, учитывающая «взрывной» трафик
- Оптимизация качества обслуживания сервисов в режиме реального времени и в зависимости от контекста
- Быстрое развертывание и конфигурирование информационных ресурсов предприятия
- Возможность быстрой костомизации сервиса
- Федерация динамических виртуальных сетей от разных операторов

Новые расширенные услуги

- Контекстная оптимизация качества сервисов в режиме реального времени
- Сервисы безопасности: firewalls, IPS. IDS и безопасность конечных пользователей
- Iaas: вычисление, хранение и «рабочий стол» как сервис
- Сетевые функции как сервис (vIMS и vEPC)
- Связность подключенного предприятия: SD-VPN и виртуальные CPE сервисы

«Если в 80-е годы главным было качество, а в 90-е – реинжиниринг, то в 2000-е главное - **скорость**».

Bill Gates, Microsoft

«То, насколько быстро вы можете **адаптировать** свои цели, лучше всего характеризует вашу компанию. Поэтому надо прививать людям **вкус к переменам.** Надо говорить о переменах постоянно».

Jack Welch, General Electric

Источник: Bell Labs Alcatel Lucent «Reshaping the future with NFV and SDN», 2015

Вопросы?

ЦЕНТР ПРИКЛАДНЫХ ИССЛЕДОВАНИЙ КОМПЬЮТЕРНЫХ СЕТЕЙ

http://arccn.ru/

smel@arccn.ru

+7 (495) 240-50-63

@ArccnNews