

Санкт-Петербургский государственный университет

Кафедра системного программирования

Нижарадзе Анастасия Тимуровна

# Реализация стенда Network Function Virtualization

Курсовая работа

Научный руководитель:  
ст. преп. И.В. Зеленчук

Санкт-Петербург  
2019

# Оглавление

<b>Введение</b>	<b>3</b>
<b>1. Цель работы</b>	<b>5</b>
<b>2. Введение в предметную область</b>	<b>6</b>
2.1 Network Function Virtualization	6
2.1.2 Блок VNF	7
2.1.3 Блок NFVI	7
2.1.4 Блок NFV MANO	7
2.1.5 Блок OSS /BSS	8
<b>3. Примеры функций, реализуемых с помощью NFV</b>	<b>9</b>
3.1 Межсетевой экран	9
3.2 Балансировка нагрузки на сеть	9
3.3 Quality of service (QoS)	10
3.4 Маршрутизация	10
3.5 Мониторинг трафика, детектирование определенного вида трафика	10
<b>4. Обзор</b>	<b>11</b>
4.1 Обзор существующих решений	11
4.2 Обзор существующих установщиков	12
<b>5. Планируемое к реализации ПО под NFV</b>	<b>13</b>
<b>6. Перечень необходимого оборудования</b>	<b>14</b>
<b>7. Требования к виртуальным машинам</b>	<b>16</b>
<b>8. Решение проблем информационной безопасности с помощью NFV</b>	<b>17</b>
<b>9. Реализация</b>	<b>18</b>
9.1 Kernel-based Virtual Machine	18
9.2 Preboot eXecution Environment	19
<b>Заключение</b>	<b>21</b>
<b>Список литературы</b>	<b>22</b>

# Введение

В современном мире компаниям, так или иначе связанным с телекоммуникациями, приходится закупать оборудование для создания своей сетевой инфраструктуры. Однако, большинство производителей, выпускающих такого рода оборудование, не позволяют пользователю изменять программное обеспечение устройства, т. е., закупка некоторого количества сетевых коммутаторов, маршрутизаторов и т. д. влечет за собой не только последующую установку, настройку оборудования, его сопровождение, обеспечение энергетическими и географическими ресурсами, но и трудности, связанные с невозможностью обновить или заменить программное обеспечение или отдельные сетевые услуги. Это, в свою очередь, влечет за собой все более и более возрастающие финансовые траты. К тому же сети, сконструированные таким образом, мало поддаются масштабированию и тяжелы в управлении и поддержке.

**Виртуализация сетевых функций (NFV)** — это концепция сетевой архитектуры, которая предлагает использовать виртуализацию как инструмент для создания сетевых услуг, таких как Network Address Translation (преобразование сетевых адресов, NAT), firewall и т. д. Она позволяет существенно снизить затраты на обеспечение сети, т. к. при устаревании программного обеспечения или необходимости добавить новую сетевую функцию более не нужно закупать новые устройства.

Впервые в 2012 году группа ETSI ISG NFV (European Telecommunications Standards Institute Industry Specification Group for NFV) опубликовала доклад о NFV на конференции в Дармштадте, Германия по программно-определяемым сетям (SDN) и OpenFlow. В течение года ETSI опубликовала статьи о сценариях использования NFV и в 2014 году — определяющих архитектуру NFV.

В связке с SDN данная технология позволяет продуктивно мониторить сетевой трафик, а также оперативно внедрять необходимые ограничения в правила маршрутизации.

В России технология NFV пока не нашла большого распространения, практически нет опыта ее применения и отечественных реализаций. Данная курсовая работа, а также работа студента Кижнерова П.А., являются первыми исследованиями на кафедре системного программирования в этом направлении.

Реализация тестового стенда NFV позволит глубже разобраться с данной концепцией, дополнить существующие реализации своими решениями и в дальнейшем внедрить технологию на российский рынок.

# 1. Цель работы

Целью работы является реализация рабочего тестового стенда NFV. Для ее достижения были выделены следующие задачи:

- Изучить предметную область и существующие решения данной задачи по реализации NFV
- Провести сравнительный анализ этих решений и выбрать наиболее подходящее для реализации в рамках стенда NFV
- Изучить и выполнить требования по развертыванию выбранного решения, подготовить для него программное и физическое окружение
- Реализовать выбранное решение, а также реализовать в тестовом виде некоторые виртуальные функции

Для установки подходящего решения требуются некоторые навыки администрирования, поэтому были выделены следующие подзадачи:

- Изучение работы гипервизора
- Изучение технологии PXE (Preboot eXecution Environment)

## 2. Введение в предметную область

### 2.1. Network Function Virtualization

**Network Function Virtualization (NFV)** — это концепция сетевой архитектуры, представленная в 2012 году европейским институтом телекоммуникационных стандартов (ETSI) [1], буквально — виртуализация сетевых функций. Стандарт NFV, предложенный ETSI, описывает инфраструктуру, внедрение которой позволит перенести сетевые функции в виртуальное пространство для легкого и удобного предоставления телекоммуникационных услуг.

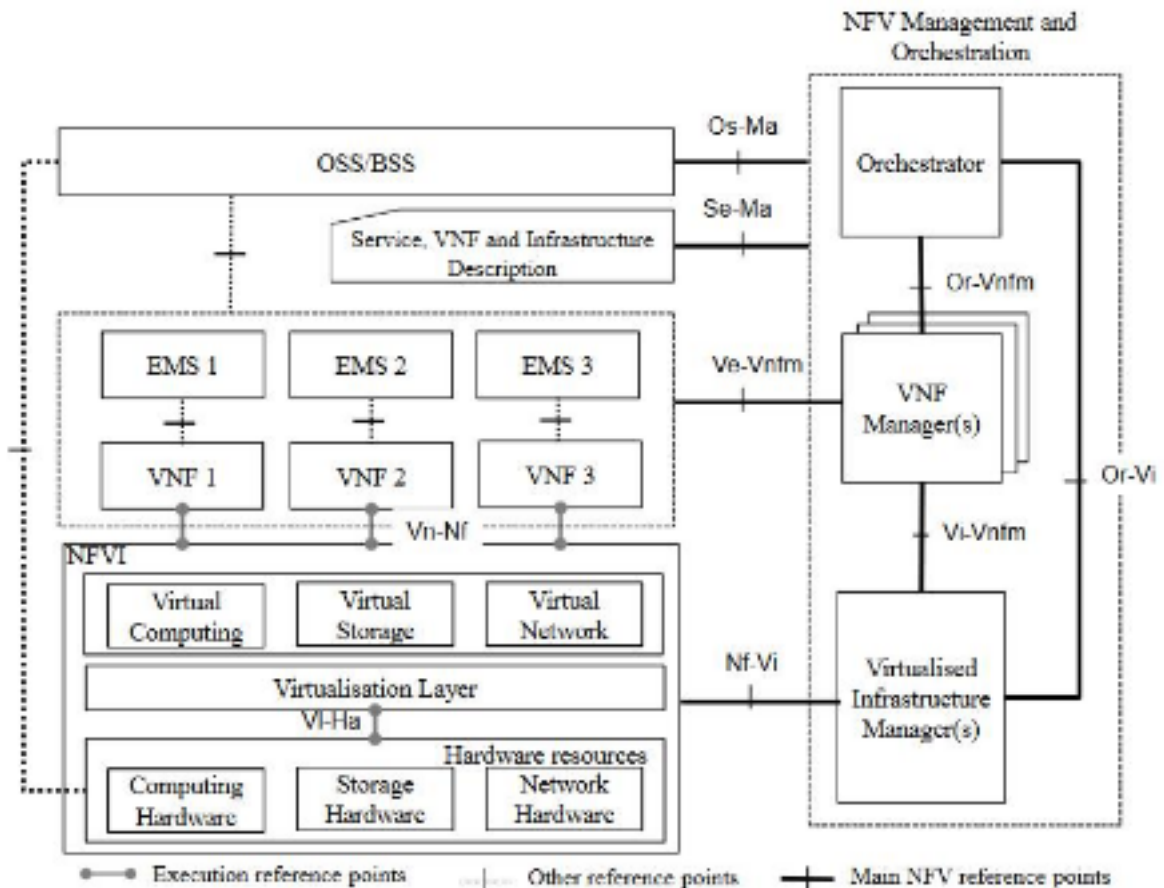


рис.1 Архитектура NFV

На рисунке 1 представлена архитектура NFV, разработанная ETSI. Как видно из рисунка, она разделена на 4 логических блока: NFV MANO — менеджер и оркестратор NFV, NFVI — инфраструктура NFV, VNF — виртуальные сетевые функции и OSS /BSS — система поддержки операций и бизнеса. Они соединены референсными точками: в отличие от интерфейсов, которые подразумевают обмен данными между объектами, референсные точки определяют взаимодействие между функциональными архитектурными блоками.

### **2.1.1. Блок VNF**

Виртуальные сетевые функции VNF (Virtual Network Function) являются основой всей архитектуры. Это функции сетевых элементов, которые могут быть представлены программно в NFV (например NAT, firewall и т. д.).

Система администрирования элементов EMS (Element Management System) предназначена для администрирования VNF, т. е. управления при отказах, управления конфигурацией, производительностью, обеспечения безопасности и учета через закрытые референсные точки.

### **2.1.2. Блок NFVI**

Инфраструктура NFVI (Network Function Virtualization Infrastructure) включает в себя физические и виртуальные ресурсы, а также плоскость виртуализации, находящуюся между ними.

Виртуальные ресурсы делятся на вычислительные, сетевые и ресурсы хранения. На них работают Виртуальные сетевые функции VNF.

Плоскость виртуализации (Virtualization Layer) отвечает за абстрагирование физических ресурсов при помощи гипервизора.

Аппаратные ресурсы делятся на вычислительные, сетевые и ресурсы хранения. На них запускаются виртуальные ресурсы.

### **2.1.3. Блок NFV MANO**

NFV менеджер и оркестратор NFV MANO (NFV Management & Orchestration) представляет собой программное решение для предоставления сетевых сервисов OSS /BSS и менеджмента VNF, инфраструктуры NFV и

жизненного цикла телекоммуникационных услуг. NFV MANO состоит из трех частей: Менеджер VNFM, Менеджер виртуализированной инфраструктуры VIM и Оркестратор NFV (NFV Orchestrator).

Менеджер VNFM (VNF Manager) управляет работой VNF: инсталляция, активация, масштабирование, обновление и терминирование. В отличие от EMS, VNFM администрирует VNF по открытым референсным точкам.

Менеджер виртуализированной инфраструктуры VIM (Virtualized Infrastructure Manager) отвечает за администрирование инфраструктуры NFVI. В его задачи также входит управление жизненным циклом виртуальных ресурсов и сбор результатов измерений производительности.

Оркестратор NFV (NFV Orchestrator) выполняет две основные функции: оркестрацию ресурсов и оркестрацию услуг. Первое подразумевает под собой некую координацию ресурсов инфраструктуры, их занятие и освобождение с помощью референсных точек посредством менеджера инфраструктуры. Второе же предназначено для управления виртуальными функциями и объединения их в комплексные услуги.

#### **2.1.4. Блок OSS /BSS**

Система поддержки операций и бизнеса OSS /BSS (Operation Support System /Business Support System) - это некая система оператора, занимающаяся администрированием сети, которая должна быть интегрирована в NFV посредством открытых референсных точек для управления сетью с помощью оркестратора.



## **3. Примеры функций, реализуемых с помощью NFV**

### **3.1. Межсетевой экран**

**Межсетевой экран** — это комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях модели OSI в соответствии с заданными правилами. Сетевые устройства со встроенным межсетевым экраном стоят гораздо дороже, чем аналогичные устройства без данной сетевой функции. Если сеть не статична, т. е. время от времени в ней появляются новые устройства, то рано или поздно придется закупать и новые маршрутизаторы с межсетевыми экранами. Реализация данной сетевой функции в NFV позволит избежать такой проблемы, т. к. становится возможным при необходимости добавлять или убирать требуемые виртуальные функции, а не покупать дорогостоящее оборудование.

### **3.2. Балансировка нагрузки на сеть**

**Балансировка нагрузки на сеть** — это метод распределения нагрузки между несколькими вычислительными ресурсами и/или сетевыми устройствами для повышения пропускной способности сети, уменьшения времени отклика и предотвращения перегрузки какого-либо одного ресурса. Динамический подбор весов балансировщика — достаточно сложная задача, требующая много ресурсов процессора, поэтому целесообразно использовать данный метод в связке с NFV. Это позволит управлять нагрузкой всей сети, при этом не загружая сетевые устройства.

### **3.3. Quality of service (QoS)**

**Quality of service (QoS, качество обслуживания)** — технология предоставления различным классам трафика различных приоритетов в обслуживании. Технология QoS — достаточно ресурсоёмкая и весьма существенно грузит процессор. И тем сильнее грузит, чем глубже в заголовки приходится залезать для классификации пакетов. Соответственно, выставление приоритетов пакетов на коммутаторах будет существенно менее производительно, чем на серверах NFV.

### **3.4. Маршрутизация**

**Маршрутизация** — процесс определения наилучшего маршрута, по которому пакет может быть доставлен получателю. Виртуальная маршрутизация позволит добавлять и убирать хосты из сети по мере надобности из одного пункта управления путем перенастраивания таблиц маршрутизации, а также позволит уменьшить время задержки благодаря переносу вычислений в ЦОД (Центр Обработки Данных).

### **3.5. Мониторинг трафика, детектирование определенного вида трафика**

В SDN/NFV сетях весь трафик проходит через NFVI уровень. Это означает, что с той или иной степенью детализации можно контролировать пакеты, проходящие через сеть. Например, администратор NFV может настроить зонд для наблюдения в режиме реального времени с высокой степенью детализации определенных метаданных, например анализировать заголовки или даже содержимое пакетов. Из этого следует возможность детектирования и сбора определенного вида трафика. Это может качественно улучшить контроль над сетью и, соответственно, ее безопасность.

## 4. Обзор

### 4.1. Обзор существующих решений

Реализация стенда NFV предполагает настройку инфраструктуры программного и аппаратного обеспечения (т. е. NFVI и VIM), а также развертывание и настройку оркестратора услуг и менеджера виртуальных функций (т.е. VNFM и Orchestrator). На данном этапе работы над курсовой было принято решение сконцентрировать усилия на реализации инфраструктуры и ее менеджменте, т. к. оркестрация без инфраструктуры не представляется возможной. Был проведен сравнительный анализ существующих реализаций VIM и NFVI и выбрана одна наиболее подходящая под текущую задачу.

**VMware vCloud NFV** [2] — это модульная платформа, главной задачей которой является виртуализация и администрирование инфраструктуры, соответствующей стандартам ETSI. Данное решение отлично интегрируется под разные платформы, легко в настройке и управлении, однако совершенно не подходит под нашу задачу, т. к. код платформы проприетарен, закрыт и сам продукт платный, свои решения в него также невозможно добавить.

**OPNFV** [3] — это крупный проект консорциума The Linux Foundation, направленный на разработку компонентов NFV в открытых экосистемах. Он также полностью основан на стандартах ETSI. Это проект с открытым программным кодом, распространяющийся под лицензией Apache [4], а также с большим выбором релизов и сценариев под разные задачи, так что данное решение отлично подходит для реализации тестового стенда.

Из существующих релизов был выбран именно Gambia [5] как самый новый и стабильный из всех на момент выбора релиза.

Каждый релиз может быть установлен разными установщиками и по разным сценариям. Для того, чтобы выбрать оптимальный установщик,

поддерживающий установку на аппаратное обеспечение, и сценарий, было выполнено детальное сравнение существующих вариантов.

## 4.2. Обзор существующих установщиков

**Apex** [6] — установщик, использующий для развертывания менеджера инфраструктуры VIM TripleO от Redhat. Его безусловными плюсами являются возможность обновления без переустановки операционной системы, одинаковые операционные системы на Jump Host и на узлах и одинаковый интерфейс для загрузки по сети с помощью PXE и Openstack admin /MGMT network. Однако, Apex не поддерживает перезагрузку Jump Host'a и в узлах невозможно пользоваться правами администратора.

**Compass4NFV** [7] — установщик, у которого слабая поддержка, сложная установка и большие требования к аппаратному обеспечению сервера.

**Fuel** [8] — установщик с хорошей документацией, минимальными требованиями к аппаратному обеспечению, автоматической установкой SSH ключей и поддержкой перезагрузки Jump Host'a.

Исходя из ограничений, существующих в рамках нашей задачи, Fuel был выбран как наиболее подходящий установщик для реализации стенда NFV.

Каждый установщик для каждого поддерживаемого им релиза предоставляет он ему несколько сценариев развертки [9]. Учитывая выбранные нами релиз и установщик, а также архитектуру процессора сервера и необходимость развернуть самую базовую сборку тестового стенда, нами был выбран сценарий os-nosdn-nofeature-noha.

## 5. Планируемое к реализации ПО под NFV

В данный момент существуют готовые решения с открытым исходным кодом для основных функциональных блоков архитектуры NFV:

- 1) Инфраструктура для виртуализированных сетевых функций предоставляется гипервизором KVM,
- 2) Менеджер виртуальной инфраструктуры реализуется средствами OpenStack, входящими в OPNFV,
- 3) Оркестратор NFV разрабатывается многими организациями, такими как ONAP, OSM, OpenBaton

Многие компании также предоставляют готовые виртуализированные сетевые функции, совместимые с конкретными оркестраторами. Например A10 vThunder предоставляет операторам сетей OSM-совместимую виртуальную функцию ADC (Application Delivery Controller), которая балансирует нагрузку на сервере.

Таким образом, готовые решения для всех компонентов архитектуры NFV существуют в зависимости от цели использования NFV. Однако, для создания контролируемой сети необходимо реализовать собственную виртуальную функцию мониторинга трафика и детектирования трафика специфичного вида, ввиду отсутствия реализации таковой.

## 6. Перечень необходимого оборудования

Наименование устройства	Технические параметры	Кол-во
Сервер (Контроллер SDN)	<p>описание: <b>Материнская плата</b>  продукт: P8Z77-V PRO  производитель: ASUSTeK COMPUTER INC.  производитель: American Megatrends Inc.</p> <p>описание: <b>ЦПУ</b>  продукт: Intel(R) Xeon(R) CPU E3-1220 V2 @ 3.10GHz  производитель: Intel Corp.  физический ID: 4  сведения о шине: cpu@0  версия: Intel(R) Xeon(R) CPU E3-1220 V2 @ 3.10GHz  слот: LGA1155  размер: 2394MHz  capacity: 3800MHz  разрядность: 64 bits  частота: 100MHz  возможности: x86</p> <p><b>RAM:</b> 10 Gb.  <b>ROM:</b> 300 Gb.</p>	1
Сервер (сервисы и приложения).	<p>описание: <b>Материнская плата</b>  продукт: P8Z77-V PRO  производитель: ASUSTeK COMPUTER INC.  производитель: American Megatrends Inc.</p> <p>описание: <b>ЦПУ</b>  продукт: Intel(R) Xeon(R) CPU E3-1220 V2 @ 3.10GHz  производитель: Intel Corp.  физический ID: 4  сведения о шине: cpu@0</p>	1

	<p>версия: Intel(R) Xeon(R) CPU E3-1220 V2 @ 3.10GHz  слот: LGA1155  размер: 2394MHz  capacity: 3800MHz  разрядность: 64 bits  частота: 100MHz  возможности: x86</p> <p><b>RAM:</b> 16 Gb.  <b>ROM:</b> 300 Gb.</p>	
SDN коммутатор (Mikrotik)	Mikrotik RB 201 1UI AS-RM	3
SDN коммутатор (Zelax)	ZES v.3028GPX	2

## 7. Требования к виртуальным машинам

	OpenStack (платформа)			SDN
Название	OpenStack Controller	OpenStack Compute	OpenStack Network	SDN Controller
Число ядер	8	4	2	4
Оперативная память, ГБ	16	8	8	12
Жесткий диск, ГБ	100	100	80	80



## **8. Решение проблем информационной безопасности с помощью NFV**

Исторически интернет развивался людьми, которые не преследовали цель контролирования сети. Это привело к тому, что сегодня интернет представляет из себя свободное пространство, где происходит множество правонарушений, так как нет эффективных инструментов их обнаружения, таких как анализ сетевого трафика из-за того, что внедрение дополнительных аппаратных решений существенно отразится на стоимости масштабирования и сопровождения сети.

NFV позволяет повысить уровень масштабируемости виртуальной сети и эффективно распределять ее ресурсы. Ввиду этого появляется возможность направлять существенную часть вычислительной мощности на конкретные задачи, такие как анализ сетевого трафика, проходящего через виртуальную инфраструктуру. Можно выделить два подхода: акцент на количественную обработку, либо на качественную; либо система занимается тривиальным анализом существенного количества трафика, либо производится более глубокий анализ пакетов. Таким образом, есть возможность найти компромисс между объемом и уровнем сложности так, что анализ сетевого трафика будет производиться максимально возможным эффективным образом и без внедрения специального физического оборудования.

## 9. Реализация

Для установки Gambia с помощью Fuel необходимо выполнить требования [8] к программному и аппаратному обеспечению. Для этого на сервер была установлена операционная система CentOS 7, изучен и установлен гипервизор KVM (Kernel-based Virtual Machine), а также изучена и применена технология PXE (Preboot eXecution Environment).

### 9.1. Kernel-based Virtual Machine

**KVM** — программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86.

В качестве плоскости виртуализации NFVI, выбранный нами установщик использует гипервизор KVM. Чтобы начать работу с VIM, необходимо было изучить данную технологию. Эту часть работы в большей степени выполнял Павел Кижнеров, в тексте его курсовой можно найти более подробное описание изученного материала.

На операционную систему CentOS 7 были установлены следующие пакеты и пакеты, им необходимые:

Название пакета	Пояснение
qemu-kvm	Гипервизор
libvirt	Библиотека для управления виртуализацией
virt-install	Менеджмент виртуальных машин
bridge-utils	Настройка сетевых мостов
tiger-vnc	Настройка VNC-сервера

После запуска KVM необходимо было настроить виртуальную сеть для доступа виртуальных машин к хост-узлу и внешней сети. Для этого была

проведена настройка конфигурационных файлов сетевого адаптера и сетевого моста(`ifcfg-enp4s0f0` и `ifcfg-br0` соответственно) и перенаправление сетевого трафика через мост.

Следующим шагом было создание виртуальной машины с помощью команды `virt-install`. В качестве гостевой операционной системы была выбрана `ubuntu16.04`, т.к. она есть в списке поддерживаемых, наиболее знакома и проста в управлении.

Для завершения установки и последующего доступа к виртуальной машине на компьютере администратора был установлен VNC-клиент. Для этого было произведено подключение к виртуальной машине через те `ip`-адрес и порт, на которых слушает трафик виртуальная машина.

## 9.2. Preboot eXecution Environment

Для установки операционных систем на виртуальные машины скрипт установщика `Fuel deploy.sh` использует технологию PXE. Перед началом развертывания тестового стенда необходимо было изучить данную технологию. Эта часть работы была более подробно изучена мной.

**PXE** — среда для загрузки компьютеров с помощью сетевой карты без использования жёстких дисков и других устройств, применяемых при загрузке операционной системы.

Первым шагом настройки PXE-сервера была настройка TFTP сервера. Для этого были установлены необходимые пакеты `tftp` и `tftpd-hpa`, и затем в созданную папку `/tftpboot` скачан загрузчик `syslinux`. Этот загрузчик был выбран как самый популярный и простой в настройке. Далее была проведена настройка конфигурационного файла `tftpd-hpa`.

Затем необходимо было настроить DHCP-сервер. Для этого был установлен пакет `isc-dhcp-server`, и затем в конфигурационный файл `isc-dhcp-server` прописать имя интерфейса, на котором DHCP-сервер будет обслуживать запросы. Далее необходимо было настроить конфигурационный файл `dhcpd.conf`, чтобы сервер мог выдавать `slave`-машинам `ip`-адреса, а также `ip`-адреса шлюза и DNS-серверов. Также в конфигурационный файл было добавлено имя загрузчика для PXE загрузки `slave`-машин.

Далее был загружен образ ubuntu16.04, т.к. для тестирования работы PXE не принципиален выбор операционной системы; затем была произведена настройка boot-меню: в конфигурационном файле загрузчика добавлен вариант загрузки этой операционной системы, а также произведена базовая настройка интерфейса загрузки.

# Заключение

В ходе выполнения курсовой работы были достигнуты следующие цели:

- Изучены предметная область и существующие решения
- Проведен сравнительный анализ этих решений и выбрано наиболее подходящее
- Изучена работа гипервизора KVM
- Изучена технология PXE

# Список литературы

- [1] Network Functions Virtualisation (NFV); Architectural Framework  
ETSI GS NFV 002 V1.2.1 (2014-12) — URL :  
[https://www.etsi.org/deliver/etsi\\_gs/NFV/001\\_099/002/01.02.01\\_60/gs\\_NFV002v010201p.pdf](https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf)
- [2] VMware documentation to vCloud NFV — URL :  
<https://docs.vmware.com/en/VMware-vCloud-NFV/3.0/vmware-vcloud-nfv-30/GUID-F8BB7D84-A9A6-4A8F-8124-2E80DF82DF48.html>
- [3] OPNFV Platform Overview — URL :  
<https://www.opnfv.org/software/technical-overview>
- [4] Licensing in OPNFV — URL :  
<https://wiki.opnfv.org/display/DEV/Licensing+in+OPNFV>
- [5] “Gambia” release of OPNFV — URL :  
<https://wiki.opnfv.org/display/SWREL/Gambia>
- [6] OPNFV Installation instructions (Apex) — URL :  
<https://opnfv-apex.readthedocs.io/en/stable-gambia/release/installation/index.html#apex-installation>
- [7] OPNFV Installation instructions (Compass4NFV) — URL :  
<https://opnfv-compass4nfv.readthedocs.io/en/stable-gambia/release/installation/index.html#compass4nfv-installation>
- [8] OPNFV Installation instructions (Fuel) — URL :  
<https://opnfv-fuel.readthedocs.io/en/stable-gambia/release/installation/installation.instruction.html#>
- [9] Gambia Scenario Status — URL :  
<https://wiki.opnfv.org/display/SWREL/Gambia+Scenario+Status>