Известия Гомельского государственного университета
имени Ф. Скорины, № 6 (153), 2025

УДК 004.94 EDN: KQNSVY

Настройка виртуального сетевого стенда в режиме вложенной виртуализации

А.В. Воруев[1], О.М. Демиденко[1], Д.С. Сыч[1], Е.В. Рафалова[1], Д.Н. Терещенко[1], А.Г. Уймин[2], К.А. Вытовтов[3], Е.А. Барабанова[3]

В статье рассматривается подход к реализации рабочего места специалиста по тестированию иерархической модели виртуальной сетевой инфраструктуры. Предлагаются решения по оперативному контролю расхода ресурсов, устранению конфликтов и программных ограничений по сложности моделируемых систем.
Ключевые слова: гипервизор, виртуальная машина, вложенная виртуализация.

The article describes an approach to implementing a workplace for specialists testing hierarchical models of virtual network infrastructure. The solutions are proposed for operational control of resource consumption, conflict resolution, and software limitations based on the complexity of the modeled systems.
Keywords: hypervisor, virtual machine, nested virtualization.

Введение. Применение виртуальных или виртуализированных сетевых стендов является обычной практикой решения сетевых задач на предприятии при переходе на облачные сервисы. Использование технологии виртуализации требует выделения специализированного дорогостоящего оборудования, поэтому для планирования структуры стенда, отладки технических приемов и обучения специалистов возникает необходимость виртуализировать саму площадку развертывания платформы виртуализации, то есть увеличить уровень виртуализации сетевого стенда [1].

Предлагаемый виртуальный стенд предоставляет организаторам процесса обучения или разработчикам конкурсных заданий на специализированных мероприятиях удобные инструменты для управления процессом виртуализации. Они смогут оперативно изменять задания, настраивать топологии сетей и управлять доступом участников. Интеграция с внешними сервисами обеспечивает необходимый уровень актуализации данных и возможность использования популярных инструментов сетевой диагностики, мониторинга и обеспечения информационной безопасности. Поддержка облачного и локального развертывания позволяет сетевому стенду работать в разнообразных условиях, обеспечивая надежность и масштабируемость.

1. Обоснование необходимости виртуализации. Разработка виртуального сетевого стенда для проведения учебного процесса или конкурсных мероприятий является актуальной задачей в условиях развития требований к технической части обеспечения сетевым трафиком производственной сферы и цифровизации образовательного процесса. Мероприятия по оценке навыков играют важную роль в подготовке специалистов, предоставляя учащимся или участникам конкурса возможность применять теоретические знания в решении практических задач, моделирующих реальные рабочие сценарии.

Традиционные методы проведения мероприятий по оценке знаний связаны с высокими затратами на организацию, включая аренду оборудования, транспортировку участников к конкурсной площадке или специализированной лаборатории и настройку физической инфраструктуры. Кроме того, использование реального оборудования ограничивает возможности масштабирования конкурсов, так как требует значительных ресурсов и времени на оборудование дополнительных рабочих мест.

Виртуальный сетевой стенд позволяет решить эти проблемы за счет перехода в цифровую среду, где все процессы, от настройки топологий до оценки заданий, могут быть выполнены в рамках эмуляции работы сетевого стенда средствами виртуализации. В результате сокращаются не только затраты на проведение мероприятий, но и появляется возможность сделать их доступными для большего числа участников, независимо от их географического расположения.

С учетом быстро меняющихся требований к компетенциям специалистов, виртуальный стенд предоставляет возможность организаторам оперативно адаптировать задания под современные стандарты и новые технологии. Это особенно важно для подготовки участников к решению реальных профессиональных задач, с которыми они могут столкнуться в будущем. Кроме того, виртуальная среда обеспечивает равные условия для всех конкурсантов, минимизируя влияние внешних факторов, таких как качество оборудования или неполадки, которые могут возникнуть при использовании реальных физических устройств.

Технические требования к сетевому стенду следующие:

– поддержка эмуляции различных типов сетевых устройств (маршрутизаторы, коммутаторы, серверы, клиентские устройства);

– достижимые требования к оборудованию рабочего места;

– совместимость программной платформы с промышленными образцами программного обеспечения для реализации сетевой диагностики, мониторинга и обеспечения информационной безопасности;

– облачное или локальное развертывание.

Пример базовой топологии стенда представлен на рисунке 1.

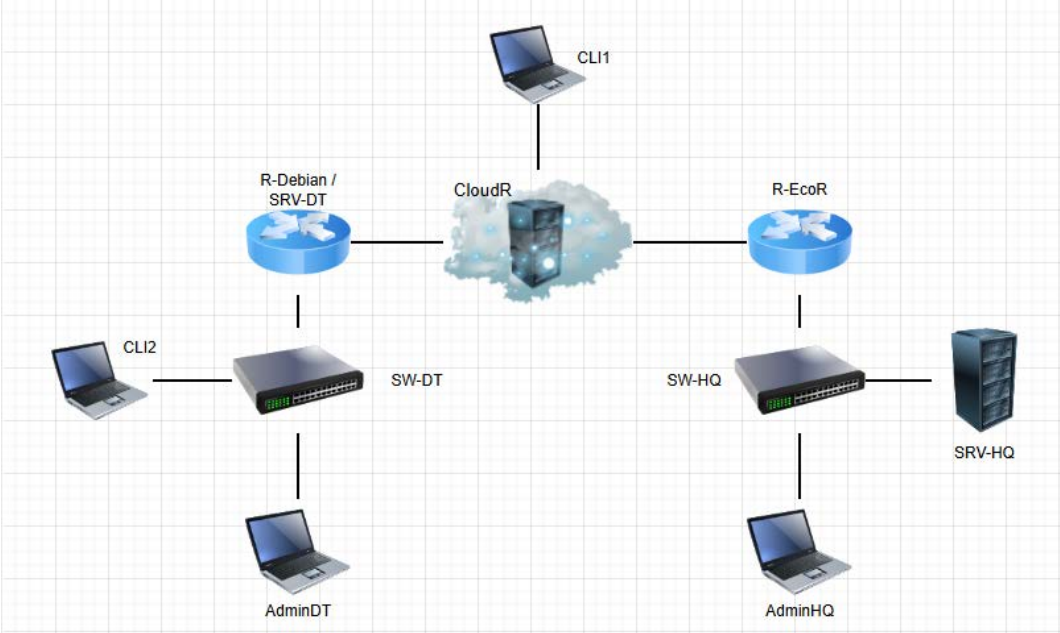

Рисунок 1 – Примерный макет топологии виртуализированной сети

В структуре топологии представлены следующие виртуальные машины:

– четыре виртуальных машины реализации сетевых сервисов, в том числе маршрутизации сетевого трафика, его фильтрации, туннелирования, выдачи сетевых параметров;

– виртуальная машина SW-HQ для продвижения сетевого трафика L2 на платформе Open vSwitch;

– две гостевые операционные системы с графическим интерфейсом AdminDT и AdminHQ для проверки доступности настраиваемых сетевых сервисов;

– две облегченные гостевые операционные системы CLI1 и CLI2 для диагностики работы сетевых протоколов и корректности обеспечения защиты информационной безопасности согласно условия задачи.

Функции сетевого коммутатора SW-DT реализуются встроенными модулями виртуального сетевого коммутатора гипервизора.

2. Использование механизмов вложенной виртуализации. Основной методологией, применяемой в проекте, является использование многоуровневой виртуализации. На рисунке 2 приведена UML-диаграмма процесса взаимодействия с виртуальным стендом.

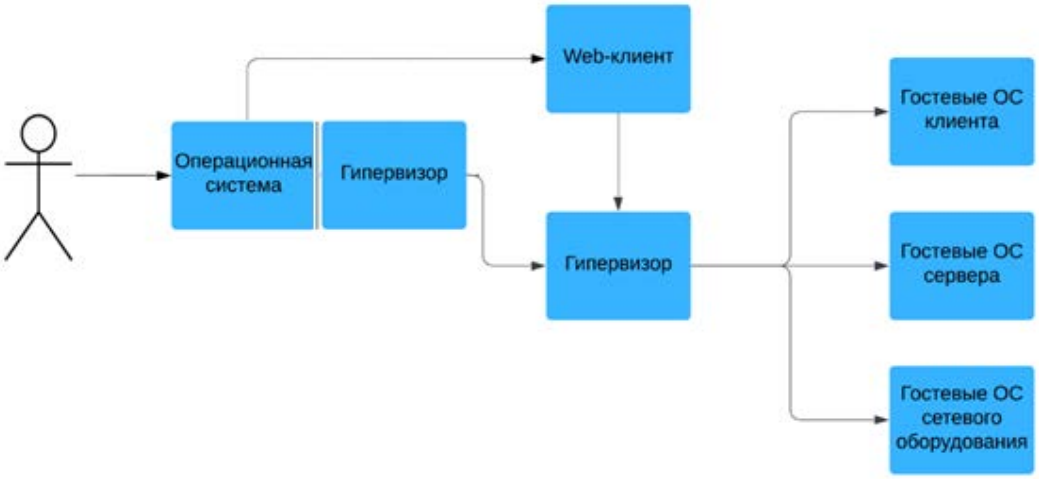

Рисунок 2 – UML-диаграмма доступа к виртуальным машинам

Процесс сборки виртуального стенда начинается с установки гипервизора Type 1 Hyper-V на родительской операционной системе Windows, после чего на его основе развёртывается web-сервис Proxmox VE [2]. Внутри Proxmox настраиваются виртуальные сети, создаются и конфигурируются гостевые операционные системы, включая клиентские машины, серверы и устройства сетевой инфраструктуры. Пользователь взаимодействует с системой через web-сервис Proxmox VE, который предоставляет полный контроль над настройкой и управлением виртуальными машинами.

Предложенная модель разделяет задачи между уровнями виртуализации, что обеспечивает высокую гибкость и масштабируемость. Hyper-V функционирует как базовый уровень виртуализации, предоставляя физический доступ к аппаратным ресурсам. Поверх него устанавливается Proxmox VE, который поддерживает как контейнеры (LXC), так и полноценные виртуальные машины (KVM/QEMU). Все элементы архитектуры связаны виртуальными сетями, настраиваемыми внутри Proxmox, что обеспечивает их изоляцию и стабильность работы.

Для стабильной работы вложенный гипервизор Proxmox VE должен иметь доступ к аппаратной поддержке виртуализации на уровне CPU. Такой доступ предоставляется гипервизору серверной операционной системы в момент его активации, но дочерним операционным системам он, по умолчанию, не передается. Параметры поддержки виртуализации CPU CoreInfo следующие:

```
Intel(R) Xeon(R) CPU E5-2670  0 @ 2.60 GHz
Intel 64 Family 6 Model 45 Stepping 7, GenuineIntel
Microcode signature : 00000710
HTT                 -   Hiperthreading enabled
HIPERVISOR          *   Hipervisor is present
VMX                 -   Supports Intel hardware-assisted virtualization
SVM                 -   Supports AMD hardware-assisted virtualization
X64                 *   Supports 64 -bit mode
```

Необходимо объявить флаг виртуализации в гостевую операционную систему Proxmox VE. Для этого используется PowerShell-скрипт, изменяющий свойства виртуальной машины, в частности поведение ее процессора:

```
Set-VMProcessor -VMName psb2025 -ExposeVirtualizationExtensions $true
```

Изменение параметров режима процессора в родительской операционной системе для виртуальной машины Proxmox VE показано ниже:

```
Intel(R) Xeon(R) CPU E5-2670  0 @ 2.60 GHz
Intel 64 Family 6 Model 45 Stepping 7, GenuineIntel
Microcode signature : FFFFFFFF
HTT               -   Hiperthreading enabled
HIPERVISOR        *   Hipervisor is present
VMX               -   Supports Intel hardware-assisted virtualization
SVM               -   Supports AMD hardware-assisted virtualization
X64               *   Supports 64 -bit mode

SMX               -   Supports Intel trusted execution
SKINIT            -   Supports AMD SKINIT
```

Подпись микропроцессора изменилась на FFFFFFFF, что указывает на процессорную поддержку виртуализации для дочерней машины.

Также, чтобы решить проблему с подключением внутренних виртуальных машин вложенного гипервизора Proxmox VE к внешней сети, необходимо выключить спуфинг MAC адресов в настройках виртуальной машины на гипервизоре Hyper-V, как показано на рисунке 3.

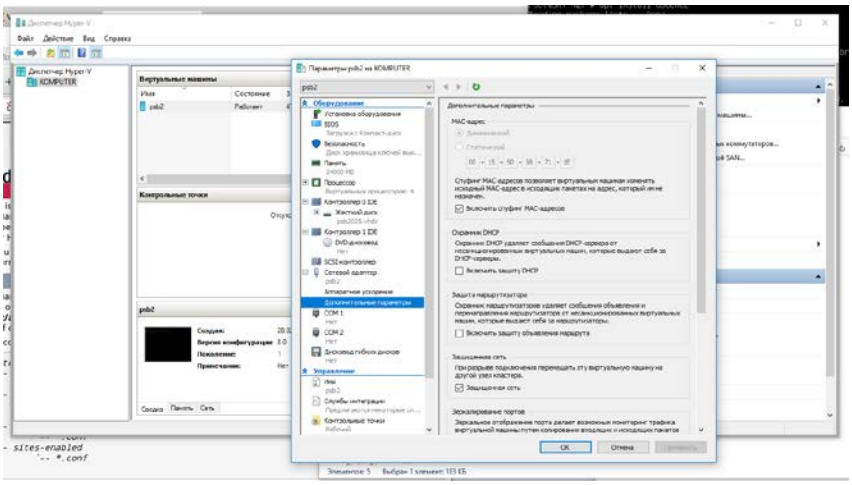

Рисунок 3 – Выключение спуфинга MAC адресов в Hyper-V

3. Настройка виртуальных машин вложенной виртуализации. Ключевой задачей обеспечения IP-связности между виртуальными машинами является реализация DHCP-сервиса [3]. В предлагаемой топологии один из сетевых сегментов обеспечивается DHCP операционной системой EcoRouter. Синтаксис его настройки имеет отличие от соседнего сегмента сети, где этот сервис настраивается для операционной системы Debian.

Пример настройки EcoRouter [4]:

```
# Создание и настройка DHCP-пула
ip dhcp pool HQ_POOL
network 192.168.11.0 /24
range 192.168.11.100 192.168.11.200
default-router 192.168.11.1
dns-server 192.168.33.1
lease 14400

# Включение DHCP-сервера на интерфейсе
interface GRO
ip address 192.168.11.1 255.255.255.0
ip dhcp server HQ_POOL
```

Схема сетевой топологии предполагает асимметричные варианты настройки сетевых машин для реализации общего сервиса, поскольку на них используются операционные системы различных производителей. Например, на устройствах R-Debian (операционная система Debian) и R-Ecor (операционная система EcoRouter) нужно настроить тоннель GRE для изолированного продвижения сетевого трафика из сегмента HQ в DT и обратно. Пример синтаксиса команд:

```
# Создание GRE-туннеля на стороне HQ R-EcoR
interface greHQ
ip add 10.10.10.1/30
ip mtu 1400
ip tunnel 192.168.11.1 192.168.33.1 mode gre

# Создание GRE-туннеля на стороне DT R-Debian
ip tunnel add greDT mode gre remote 192.168.11.1 local 192.168.33.1 ttl 255
ip addr add 10.10.10.2/30 dev greDT
ip link set greDT up.

# На R-EcoR маршрутизация трафика из HQ в DT:
ip route 192.168.33.0/24 10.10.10.2

# На R-Debian маршрутизация трафика из DT в HQ:
ip route add 192.168.11.0/24 via 10.10.10.1 dev greDT.
```

4. Проверка работоспособности и контроль расхода ресурсов. После настройки всех виртуальных машин необходимо проверить работоспособность сетевой топологии. Например, CLI1 выполняется команду для просмотра сетевых интерфейсов. Чтобы CLI1 смог получить IP адрес, необходимо также запустить CloudR, который назначает IP адрес в рамках сервиса DHCP. Далее на виртуальной машине EcoR просматривается текущее состояние устройства, а на виртуальном коммутаторе SW-HQ проверяется работоспособность функционала, реализованного с помощью Open vSwitch (рисунок 4).

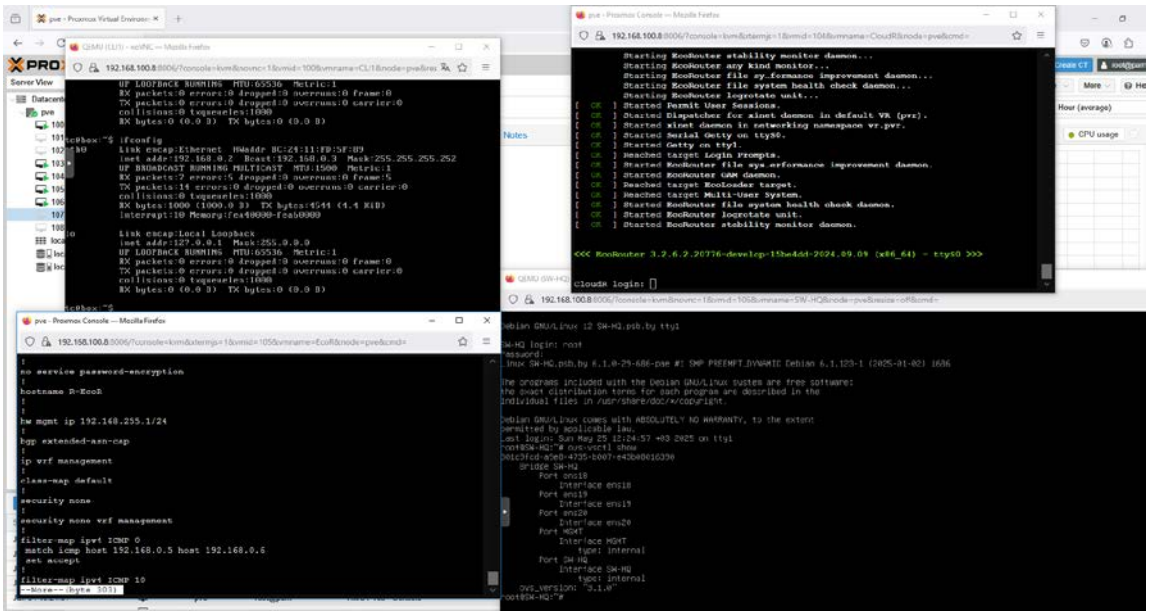

Рисунок 4 – Проверка настройки узлов CLI1, EcoR, SW-HQ

Для оценки количества ресурсов, потребляемых сетевым стендом при полностью настроенной и запущенной топологии, на платформе Proxmox используется встроенная система мониторинга. Результат показан на рисунке 5.

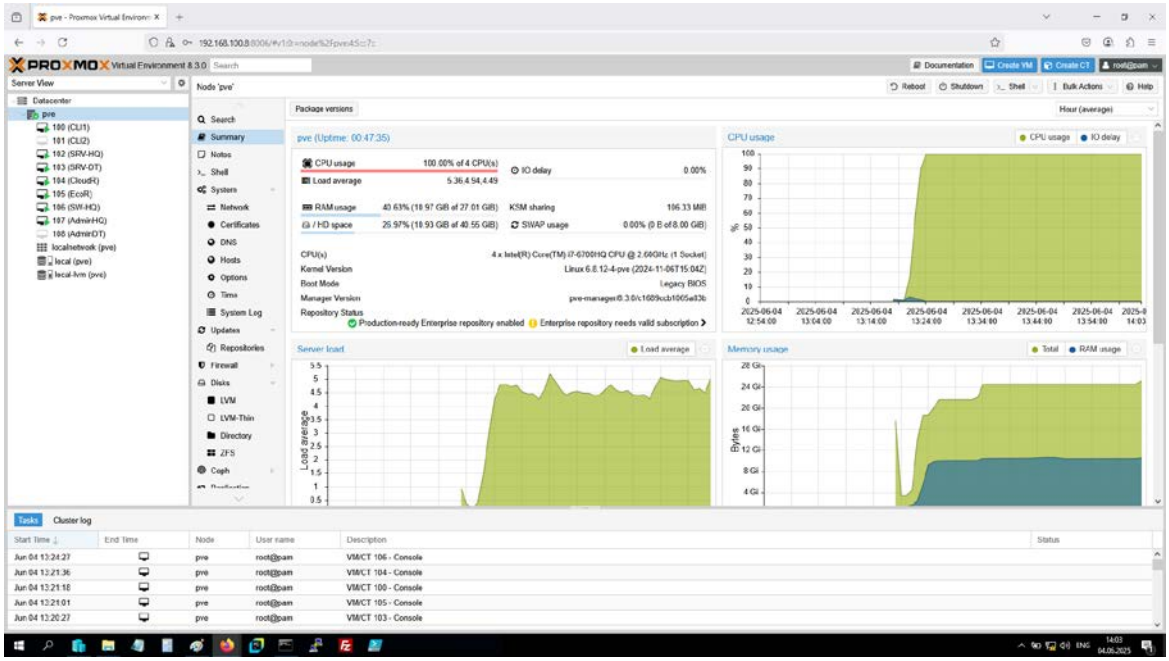

Рисунок 5 – Контроль количества потребляемых ресурсов

Заключение. В данной статье описаны подходы к разработке рабочего места для конкурсанта компетенции «Сетевое и системное администрирование» национального финала чемпионата ProfSkills Belarus 2025.

Основной методологией, применяемой в проекте, является использование многоуровневой виртуализации. В статье приведены варианты настройки виртуальных машин вложенной виртуализации. Особый интерес представляет проверка работоспособности используемой сетевой технологии и контроль расхода используемых для этого ресурсов.

Предложенные решения по использованию предлагаемого виртуального стенда предоставляют возможность организаторам оперативно адаптировать задания под современные стандарты и новые технологии.

Литература

1. Воруев, А. В. Подходы к изменению механизмов маршрутизации в сетевых структурах / А. В. Воруев, В. Д. Левчук, С. М. Колаиб // Проблемы физики, математики и техники. – 2020. – № 4 (45). – С. 121–104.

2. Воруев, А. В. Построение рабочего места для тестирования виртуальной сетевой инфраструктуры / А. В. Воруев, И. О. Демиденко, С. М. Колаиб, Д. В. Домасканов // Известия Гомельского государственного университета имени Ф. Скорины. – 2020. – № 6 (123). – С. 99–104.

3. Воруев, А. В. Программируемое управление доступом к сети с адаптивной настройкой физических интерфейсов / А. В. Воруев, И. О. Демиденко, А. И. Чернышев, С. Ю. Михневич // Известия Гомельского государственного университета имени Ф. Скорины. – 2018. – № 6 (111). – С. 55–62.

4. EcoRouter. User Guide. Руководство по установке и конфигурированию. – М. : РДП.РУ, 2018. – 349 с.

[1]Гомельский государственный
университет имени Франциска Скорины

[2]Российский государственный университет
нефти и газа имени И.М. Губкина

[3]Институт проблем
управления имени В.А. Трапезникова

Поступила в редакцию 13.10.2025