

Моделирование телекоммуникационной сети средствами сетевых инструментов Linux: инструменты создания цифровых двойников

Уймин Антон Григорьевич

старший преподаватель, Российский государственный университет нефти и газа НИУ имени И. М. Губкина, г. Москва, au-mail@ya.ru

Никитин Олег Рафаилович

доктор технических наук, профессор, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, rts@vlsu.ru

АННОТАЦИЯ

Введение: В работе осуществлено обоснование использования операционной системы Linux, как инструмент создания цифровых двойников. **Постановка задачи:** при проектировании, модернизации и тестах таких систем наиболее остро стоит проблема отсутствия сбоев в бизнес-процессе предприятия. Данная проблема решается посредством двух основных технологий: эмуляции и виртуальной инфраструктуры. KVM стал стандартом для решений по виртуализации в телекоммуникационных сетях. В частности, решения на базе Linux-серверов и сервисов (OVS, FRR) стали де-факто стандартом при решении задач виртуальной виртуализации сетей. **Методы:** анализ инструментов; методы объектно-субъектного описания информационно-телекоммуникационных систем. **Результаты:** рассмотрен Digital Twin как виртуальная модель реальной телекоммуникационной сети, которая позволяет точно представлять все ее компоненты и структуру. Рассмотренные инструменты могут быть использованы как отдельно, так и совместно для решения основных задач моделирования цифрового двойника. Нагрузка на сеть была получена в процессе обработки сетевых данных в рамках цифрового двойника телекоммуникационной сети. В этом случае следует учитывать нагрузку на центральный процессор при моделировании процессов, аналогичных работе реальной сети. Разработка реализована в рамках Чемпионата высоких технологий 2022. **Практическая значимость:** это дает возможность учесть воздействие на центральный процессор при моделировании процессов, подобных реальным сетям. Нагрузка должна определяться для сети с меньшей численностью вычислительных мощностей, чем реальная сеть. При этом будет оптимизирована нагрузка на инфраструктуру, так как появится возможность реализации виртуальной вычислительной системы. Особенно трудно при моделировании создаются службы, требования которых к работе инфраструктуры имеют значение 0.99 и обязаны иметь в наличии дополнительные вычислительные мощности. **Обсуждение:** новизна предложенных задач состоит в том, что структура подсистемы создания цифровых двойников на базе платформы linux для телекоммуникационных сетей рассматривается в системном аспекте.

КЛЮЧЕВЫЕ СЛОВА: двойник телекоммуникационной сети; сеть; виртуальный; инфраструктура; моделирование.

Введение

Телекоммуникационная сеть представляет собой сложную систему, состоящую из узлов передачи данных, стеков сетевых протоколов и источников трафика [1]. При проектировании, модернизации, а также тестировании таких систем особо остро встает вопрос отсутствия сбоев в бизнес-процессах предприятия [2]. Для решения данной задачи могут применяться две основные технологии: эмуляция и виртуализация инфраструктуры. В большинстве случаев используются комбинированные решения, обеспечивающие оптимальное соотношение цены и качества, а также скорости развёртывания моделируемого решения. В телекоммуникационных сетях решения на базе Linux серверов, сервисов, до сетевого оборудования (OVS, FRR и т.д.). Решения в области виртуализации построенные на KVM стали стандартом де факто в решениях виртуализации телекоммуникационных сетей.

Целью работы является сравнение основных встроенных и наложенных инструментов Linux для создания цифрового двойника телекоммуникационной сети.

Определим термин «Цифровой двойник» телекоммуникационной сети как виртуальную модель реальной телекоммуникационной сети, которая обеспечивает точное представление всех ее компонентов, структуры и поведения. Данный технологический подход используется для моделирования, прогнозирования, анализа и оптимизации сетей связи [3,4,5].

Цифровые двойники телекоммуникационных сетей применяются для следующих целей:

1. Оптимизация сетевого проектирования: Цифровой двойник используется для определения оптимальных мест установки оборудования, наилучшей конфигурации сети и управления ресурсами.

2. Мониторинг и управление сетью: Цифровые двойники позволяют проводить виртуальное наблюдение за состоянием сети и определение возможных проблем, что облегчает их решение в реальном времени.

3. Планирование и прогнозирование: Цифровые двойники способствуют прогнозированию поведения сети, позволяя проводить анализ нагрузки, определять потребности в масштабировании и оценивать воздействие новых технологий.

4. Тестирование и симуляция: Цифровые двойники используются для проведения симуляций и испытаний изменений в сети, позволяя проверять планируемые изменения и анализировать их воздействие на производительность сети без риска для реальной инфраструктуры.

5. Обучение и развитие персонала: Цифровой двойник используется в качестве обучающей платформы для сотрудников телекоммуникационных компаний, позволяя им получить опыт работы с сетью в безопасной симуляционной среде.

6. Интеграция и совместимость: Цифровые двойники позволяют интегрировать различные системы и оборудование, облегчая совместимость и обмен данными между ними.

7. Оценка и снижение рисков: Использование цифровых двойников позволяет оценивать риски, связанные с изменениями в сети, и принимать меры по их снижению, такие как предотвращение сбоев и минимизация простоев.

8. Устойчивость и безопасность: Цифровые двойники используются для обеспечения надежности и безопасности телекоммуникационной сети, предоставляя возможность анализа уязвимостей и потенциальных угроз, а также позволяя протестировать решения по устранению этих проблем в виртуальной среде.

9. Энергоэффективность: Использование цифровых двойников способствует оптимизации энергопотребления телекоммуникационных сетей, позволяя анализировать и управлять энергией, расходуемой сетью, и реализовывать энергоэффективные решения.

10. Разработка новых продуктов и услуг: Цифровые двойники используются для экспериментирования с новыми продуктами и услугами, позволяя проводить исследования и разработки в виртуальной среде, а также оценивать их воздействие на существующую сеть и потребителей.

11. Соблюдение норм и стандартов: Цифровые двойники могут помочь операторам телекоммуникационных сетей следить за соблюдением норм и стандартов, таких как качество обслуживания (QoS) и требования регуляторов, проверяя, как изменения в сети могут влиять на соответствие этим критериям.

12. Управление активами и инвентаризация: Цифровые двойники могут облегчить управление активами и инвентаризацию оборудования в телекоммуникационных сетях, предоставляя точную информацию о местоположении, состоянии и характеристиках каждого компонента сети.

Концепция Linux Network Namespaces представлена в операционной системе в различных вариантах [6,7]. Общая цель Namespaces состоит в том, чтобы предложить в рамках системы, пространства имен, которые будут изолировать процессы друг от друга, посредством различных системных инструментов. Network Namespaces позволяют создавать виртуальные сетевые стеки, каждый из которых может иметь свои собственные интерфейсы, маршруты, таблицы ARP и даже собственные межсетевые экраны.

Virtual Ethernet devices - виртуальные сетевые интерфейсы (veth), представляют собой пары виртуальных сетевых интерфейсов, которые можно использовать для соединения двух сетевых пространств имен (network namespaces) или других сетевых конструкций, таких как контейнеры и виртуальные машины, в операционной системе Linux [8]. Они обеспечивают передачу пакетов между разными виртуальными сетями и создают туннель для передачи данных. Принцип работы: когда одно из устройств veth получает сетевой пакет, он автоматически передает этот пакет на другое устройство veth в паре. Это позволяет устройствам в разных сетевых пространствах имен обмениваться сетевыми пакетами, как если бы они были соединены физическим кабелем.

Ограничим работу, рассмотрением наиболее часто используемых инструментов моделирования телекоммуникационных сетей средствами iproute2 [9,10] и KVM+OVS (Kernel-based Virtual Machine и Open vSwitch) [11,12]. В таблице 1 представлено сравнение реализации Virtual Ethernet devices [13,14,15,16] для iproute2 и KVM+OVS [17,18].

Можно сделать вывод, о возможности применения инструментов как по отдельности, так и совместно при решении задач моделирования цифрового двойника телекоммуникационной сети предприятия.

Основными задачами цифровых двойников телекоммуникационных сетей являются вопросы моделирования ситуаций в рамках канального и сетевого уровня модели OSI. В таблице 2 рассмотрены основные функции канального уровня iproute2 и KVM+OVS, В таблице 3 рассмотрены основные функции сетевого уровня iproute2 и KVM+OVS

Табл. 1. Сравнение функционала

Функция / Характеристика	iproute2	KVM+OVS
Тип устройства	Виртуальные сетевые интерфейсы (veth)	Виртуальные сетевые интерфейсы (tap/tun) и Open vSwitch (OVS)
Сетевая изоляция	Network Namespaces	Виртуальные машины (VM) и Open vSwitch (OVS)
Создание интерфейсов	iproute2 CLI commands	OVS CLI команды и libvirt
Управление маршрутизацией	Встроенные средства Linux (iproute2)	Open vSwitch (OVS)
Поддержка VLAN	Да, с использованием стандартных средств Linux	Да, с использованием OVS
Производительность	Зависит от ядра Linux и настройки системы	Зависит от Open vSwitch и настройки системы
Масштабируемость	Ограничена ресурсами хоста и ядра Linux	Более масштабируемая с использованием OVS и возможностей KVM
Поддержка VXLAN	Да, с использованием стандартных средств Linux	Да, с использованием OVS
Интеграция с SDN-контроллерами	Ограничена, возможна с использованием дополнительных компонентов	Да, Open vSwitch имеет встроенную поддержку SDN-контроллеров
Мониторинг и аналитика	Встроенные средства Linux (например, ifstat, iproute2)	Open vSwitch и дополнительные инструменты, такие как sFlow, NetFlow и IPFIX
Поддержка QoS	Да, с использованием стандартных средств Linux	Да, с использованием OVS и libvirt

Табл. 2. Функции канального уровня

Функция / Характеристика	iproute2	KVM+OVS
Тип устройства	veth (Virtual Ethernet)	tap/tun и Open vSwitch
Создание мостов	Да (Linux Bridge)	Да (OVS Bridge)
Управление MAC-адресами	Да	Да
Управление VLAN	Да	Да
Транковые порты	Да	Да
Контроль доступа на основе MAC	Да	Да
Поддержка MVRP	Нет	Да
Поддержка STP/RSTP/MSTP	Да	Да
Поддержка LACP	Да	Да
Поддержка Q-in-Q	Да	Да
Поддержка IGMP Snooping	Нет	Да
Поддержка VXLAN	Да	Да
Поддержка GRE	Да	Да
Поддержка протоколов туннелирования	Да	Да
Прозрачное межсетевое экранирование	Нет	Да
Транкапсуляция Ethernet	Нет	Да
Мониторинг и аналитика	Встроенные средства Linux (например, ifstat, iproute2)	Open vSwitch и дополнительные инструменты, такие как sFlow, NetFlow и IPFIX

Табл. 3. Функции сетевого уровня

Функция / Характеристика	iproute2	KVM+OVS
IP-адресация	Да	Да
Управление маршрутизацией	Да	Да (через OVS и хост-систему)
Поддержка многоадресной рассылки (Multicast)	Да	Да
Управление VRF	Да	Нет (но можно реализовать через сетевые пространства имен)
Управление туннелями	Да	Да
Поддержка GRE	Да	Да
Поддержка VXLAN	Да	Да
Поддержка MPLS	Да	Нет
Поддержка ECMP	Да	Да
NAT (сетевой адресный перевод)	Да	Да
Поддержка QoS	Да	Да
Поддержка NetFlow/sFlow/IPFIX	Нет	Да
DHCP-сервер/клиент	Да (через дополнительное ПО)	Да (через дополнительное ПО)
Поддержка IPsec	Да (через дополнительное ПО)	Да (через дополнительное ПО)
Поддержка VRRP	Да (через дополнительное ПО)	Да (через дополнительное ПО)
Поддержка BGP	Нет (но возможно через дополнительное ПО)	Нет (но возможно через дополнительное ПО)
Поддержка OSPF	Нет (но возможно через дополнительное ПО)	Нет (но возможно через дополнительное ПО)
Поддержка RIP	Нет (но возможно через дополнительное ПО)	Нет (но возможно через дополнительное ПО)
Поддержка PIM (Protocol Independent Multicast)	Нет (но возможно через дополнительное ПО)	Нет (но возможно через дополнительное ПО)
Поддержка IGMP Snooping	Нет	Да
Поддержка IPv6	Да	Да
Поддержка IPv6-маршрутизации	Да	Да (через хост-систему)
Поддержка NPTv6 (IPv6 NAT)	Да (через дополнительное ПО)	Да (через дополнительное ПО)
Поддержка IPSLA	Нет (но возможно через дополнительное ПО)	Нет (но возможно через дополнительное ПО)
Поддержка LLDP	Нет (но возможно через дополнительное ПО)	Да
Управление трафиком	Да	Да (через хост-систему)
Поддержка DNS-сервера/клиента	Да (через дополнительное ПО)	Да (через дополнительное ПО)
Поддержка NTP-сервера/клиента	Да (через дополнительное ПО)	Да (через дополнительное ПО)

В таблице необходимо обратить внимание на принятые условности. Да (через дополнительное ПО) – принято, что данное решение встречается в телекоммуникационных сетях. Нет (но возможно через дополнительное ПО) – принято, что данное решение технически реализуемо, но не встречается в телекоммуникационных сетях.

Обзор функционала канального и сетевого уровней, позволяет слетать вывод о возможности использования решения, как в сетях предприятий, так и в сетях провайдеров. Сети центров обработки данных не рассматриваются, в виду специфики архитектуры решений.

Отметим, что применение KVM+OVS для реализации функционала сетевого уровня, является нестандартным решением. В рамках виртуализации, как правило применяются специализированные средства для работы на сетевом уровне: FRR, Quagga, Bird и OpenBGPD - это реализации протоколов маршрутизации с открытым исходным кодом для Linux и других Unix-подобных операционных систем [19]. В таблице 4 рассмотрены основные параметры, связанные с поддержкой и развитием проектов. В таблицу добавлены iproute2 и OVS для сравнения статуса актуальности решений в 2023 году.

Таб. 4. Динамика развития проектов

Характеристика разработки	FRR	Quagga	Bird	OpenBGPD	iproute2	OVS
Лицензия	GPLv2	GPLv2	GPLv2	ISC	GPLv2	Apache 2.0
Последнее обновление	Март 2023	Апрель 2016	Апрель 2021	Февраль 2022	Март 2023	Март 2023
Активность разработки	Высокая	Низкая	Средняя	Низкая	Высокая	Высокая
Количество разработчиков	20+	Менее 10	10-20	Менее 5	Неизвестно	Неизвестно
Обновления безопасности	Регулярные обновления	Редкие обновления	Регулярные обновления	Регулярные обновления	Регулярные обновления	Регулярные обновления
Поддержка новых протоколов/стандартов	Быстро	Медленно	Быстро	Медленно	Быстро	Быстро
Наличие подробной документации	Да	Нет	Да	Нет	Да	Да
Наличие коммерческой поддержки	Да	Нет	Да	Нет	Да	Да
Наличие GUI	Нет	Нет	Нет	Нет	Нет	Да
Наличие REST API	Да	Нет	Нет	Нет	Да	Да
Поддержка VRF	Да	Да	Нет	Нет	Да	Да
Поддержка VXLAN	Да	Да	Нет	Нет	Да	Да
Поддержка BGP	Да	Да	Да	Да	Нет	Да
Поддержка OSPF	Да	Да	Да	Нет	Да	Нет

Free Range Routing является наиболее перспективным продуктом в данном сегменте. В таблице 5 приведен его функционал.

Рассмотренные выше решения, можно характеризовать как стек технологий, позволяющий разворачивать сложные телекоммуникационные инфраструктуры.

На рисунке 1 приведена сеть, построенная на базе рассмотренных выше технологий. разработанная для проведения конкурса Международный чемпионат высокотехнологичных профессий Хайтек 2022 по компетенции Информационная безопасность. В рамках решение профессиональных кейсов участники из 7 стран и 12 предприятий реализовали конфигурирование, тестирование и отладку телекоммуникационной инфраструктуры.

Табл. 5 Функционал решений по маршрутизации

Функция / Характеристика	iproute2	FRR
IP-адресация	Да	Да
Управление маршрутизацией	Да	Да (через Quagga и FRRouting)
Поддержка многоадресной рассылки (Multicast)	Да	Да
Управление VRF	Да	Да
Управление маршрутами BGP	Нет	Да
Управление маршрутами OSPF	Нет	Да
Управление маршрутами RIP	Нет	Да
Поддержка IPv6	Да	Да
Поддержка VXLAN	Да	Да
Поддержка Babel	Нет	Да
Поддержка BFD	Нет	Да
Поддержка MPLS	Да	Да (через LDP и RSVP-TE)
Поддержка VxLAN-GPE	Да	Да
Поддержка EVPN	Нет	Да
Поддержка PBR (Policy-Based Routing)	Да	Да

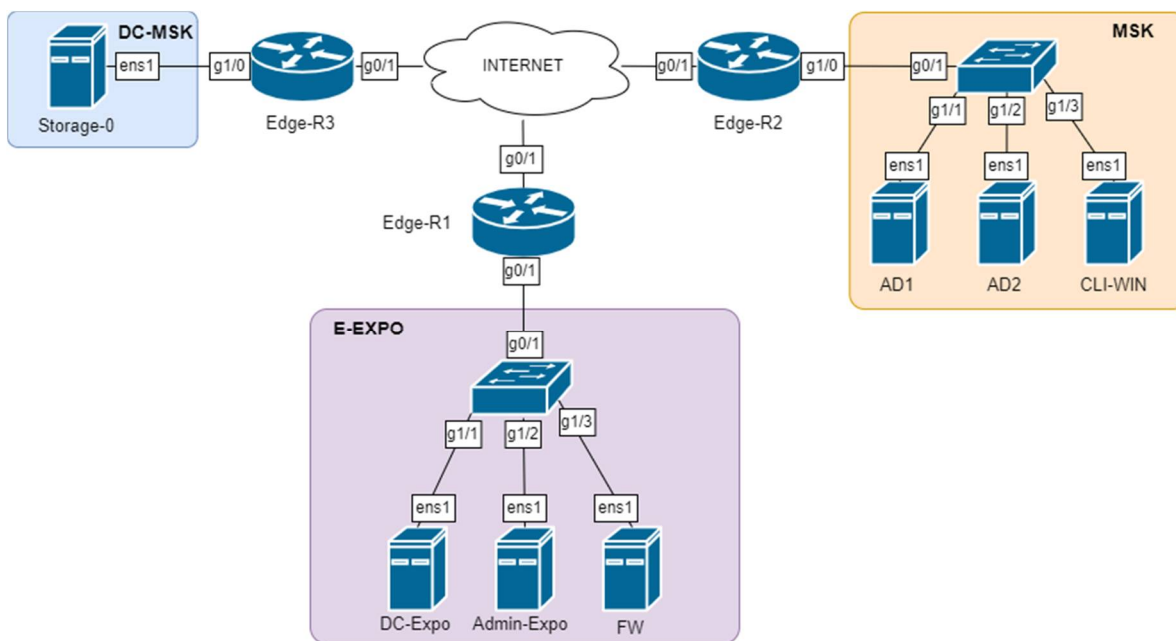


Рис. 1. Топология сети предприятия

Нагрузочное тестирование инфраструктуры, продемонстрировало возможность масштабирования решения и применения рассмотренных инструментов а рамках решения производственных задач, в том числе по импортозамещению [20].

На рисунках 2 и 3, продемонстрировано загруженность процессора и использованной оперативной памяти на nodes «PVE3». В момент работы с виртуальными машинами можно

заметить повышение загрузки процессора, колебания загрузки оперативной памяти не значительны ~2-3%.

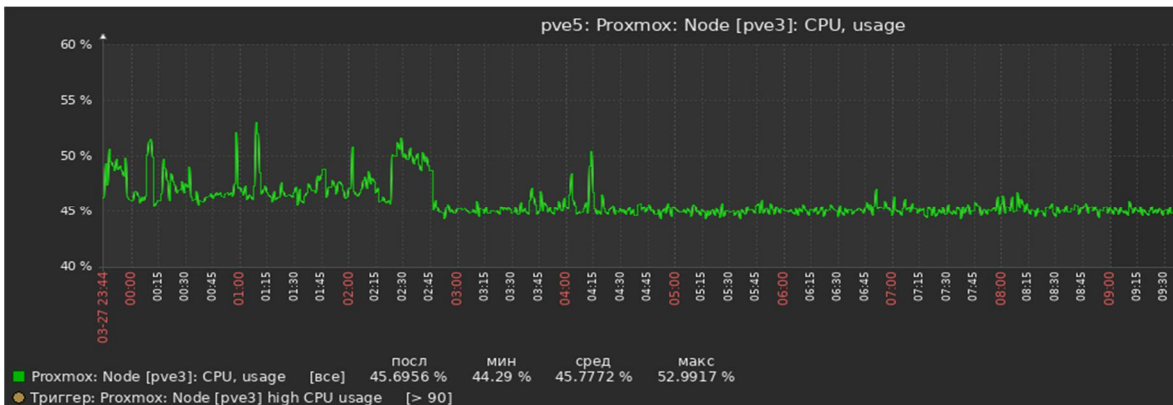


Рис. 2. Нагрузка процессора на нодах «PVE3».

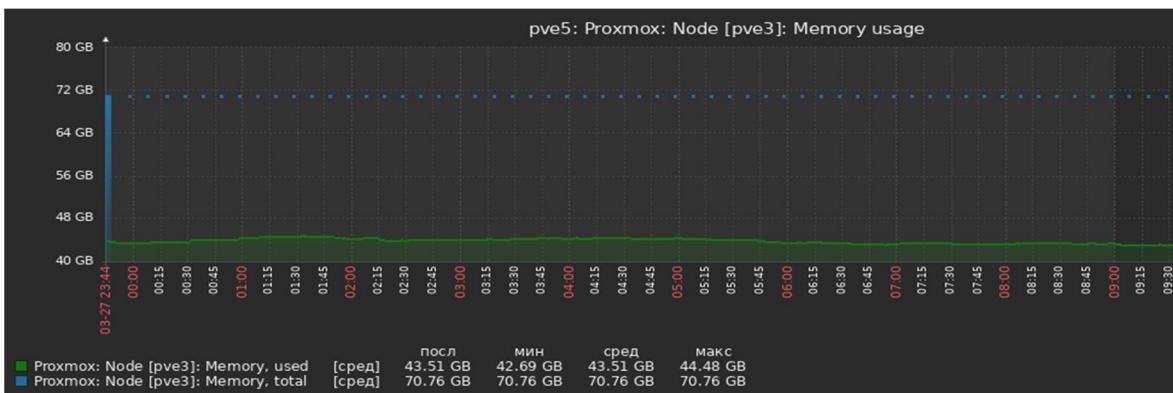


Рис. 3. Занятый объём оперативной памяти на нодах «PVE3».

На рисунках 4 и 5, продемонстрировано Загруженность процессора и использованной оперативной памяти на нодах «PVE4». В момент работы с виртуальными машинами можно заметить пики повышение загрузки процессора, колебания загрузки оперативной памяти не значительны ~2-3%.

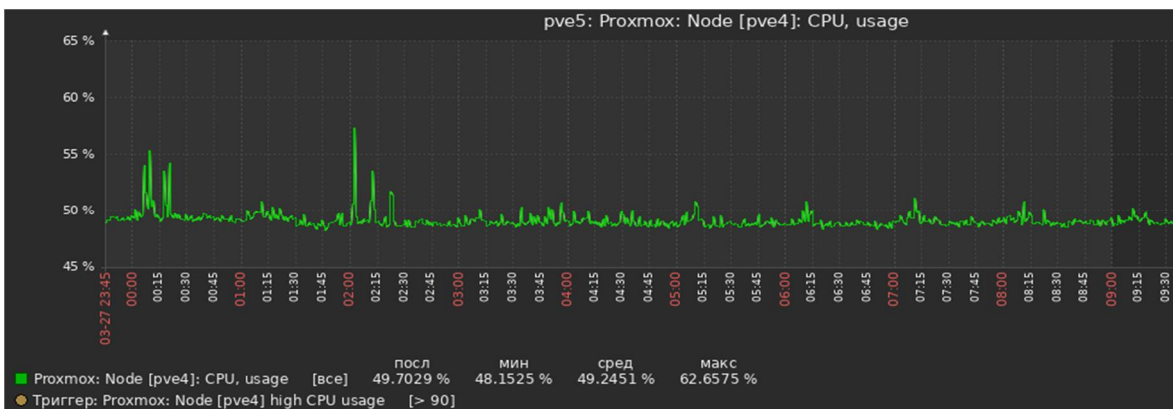


Рис. 4. Нагрузка процессора на нодах «PVE4».

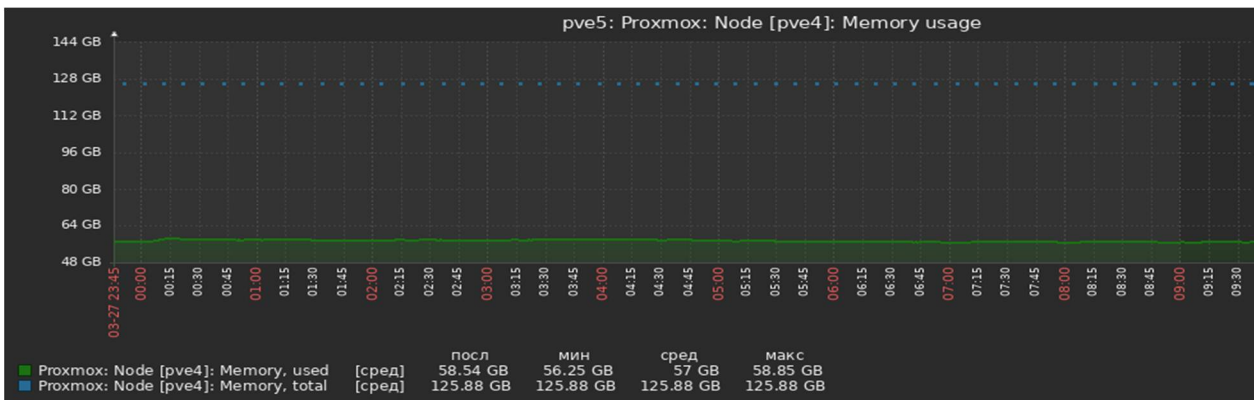


Рис. 5. Занятый объем оперативной памяти на нодах «PVE4».

На рисунках 6 и 7, продемонстрировано Загруженность процессора и использованной оперативной памяти на нодах «PVE5». На данной нодах загрузка минимальна.

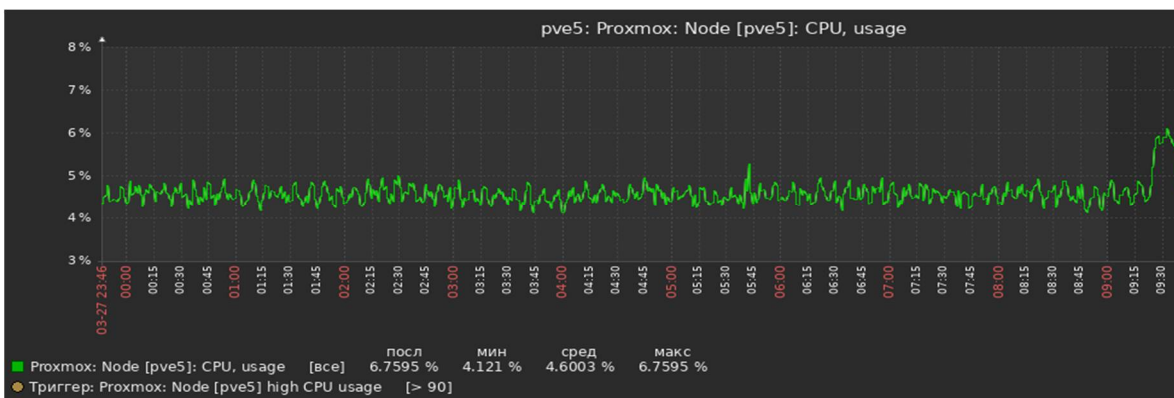


Рис. 6. Нагрузка процессора на хост «PVE5».

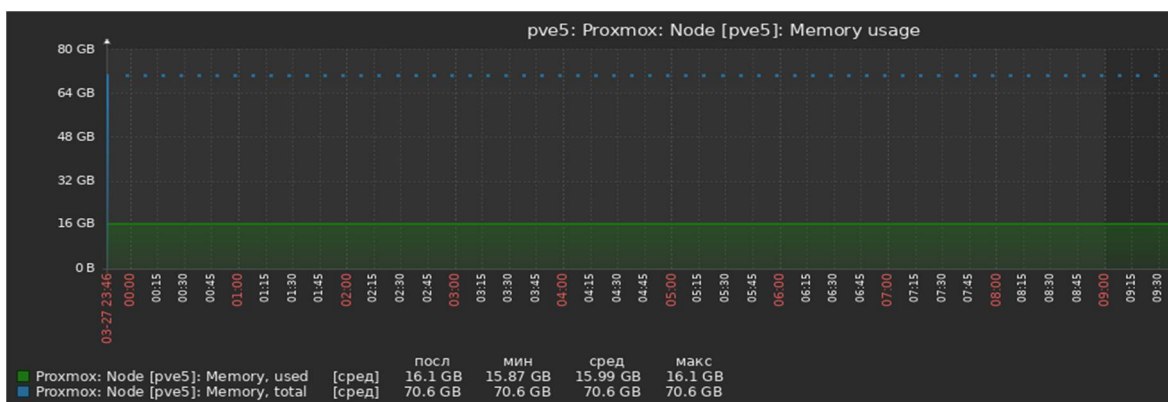


Рис. 7. Занятый объем оперативной памяти на ноде «PVE5».

Заключение

В ходе работы был проведен анализ загруженности нод гиперконвекторной системы. В процессе обработки сетевых данных в рамках цифрового двойника телекоммуникационной сети была получена нагрузка. Это позволяет учитывать нагрузку на центральный процессор при моделировании процессов, подобной работе реальной сети. Нагрузка определяется для сети с меньшим количеством вычислительных мощностей, чем реальная сеть. Это достигается за счет реализации виртуальной вычислительной системы тем самым оптимизируется нагрузка на инфраструктуру. Особую сложность при моделировании вызывают службы, у которых требования 0,99 к работе инфраструктуры, как правило должны быть обеспечены дополнительными вычислительными мощностями. В представленном цифровом двойнике телекоммуникационной сети такие службы отсутствуют.

При создании цифровой платформы была создана платформа, на которой можно организовать цифровой двойник телекоммуникационной сети. Данная разработка была реализована в рамках чемпионата Хайтек 2022. Результаты апробации кейсов были внедрены на предприятиях

Литература

1. Методы обеспечения устойчивости системы защиты информационно-телекоммуникационной сети, как динамической управляемой системы / М. А. Карпов, М. А. Коцыняк, А. П. Нечетуренко, Р. А. Перов // Состояние и перспективы развития современной науки по направлению «Информационная безопасность»: Сборник статей III Всероссийской научно-технической конференции, Анапа, 21–22 апреля 2021 года. Анапа: Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА", 2021. С. 690-696.
2. Shi J. et al. Optimization and decomposition methods in network traffic prediction model: A review and discussion //IEEE Access. 2020. Т. 8. С. 202858-202871.
3. Грищенко К. А. и др. Компьютерная модель телекоммуникационной сети объекта модульного типа, основанная на построении цифрового двойника //Актуальные проблемы инфотелекоммуникаций в науке и образовании. 2021. С. 53-58.
4. Шкарупета Е. В., Колесникова В. Б., Белянцева О. М. Мегавселенная как пространственный цифровой двойник в Индустрии 5.0. 2021. С. 96-116.
5. Махмудов, Р. Т. Анализ зашифрованного сетевого трафика с применением машинного обучения / Р. Т. Махмудов, А. Г. Уймин // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VI Региональной научно-технической конференции, посвященной 100-летию М.М. Ивановой, Москва, 19–21 сентября 2022 года. Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, 2022. С. 1133-1134.
6. Вьюгов С. Г., Козлов С. В. Анализ характеристик и возможностей виртуальной сети на основе пространств имён Network Namespace в операционной системе Gnu/Linux //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). 2022. С. 315-319.
7. Jain S. M., Jain S. M. Namespaces //Linux Containers and Virtualization: A Kernel Perspective. 2020. С. 31-43.
8. Lackorzynski T., Köpsell S., Strufe T. A comparative study on virtual private networks for future industrial communication systems //2019 15th IEEE International Workshop on Factory Communication Systems (WFCS). IEEE, 2019. С. 1-8.
9. Pandi S. et al. Networking tools //Computing in Communication Networks. Academic Press, 2020. С. 431-456.
10. Rai S. S., Monis L., Tahiliani M. P. NeST: Network Stack Tester //Proceedings of the Applied Networking Research Workshop. 2020. С. 32-37.

11. *Bazai S. U. et al.* Kernel virtual machine based high performance environment for grid and jungle computing //2021 2nd International Informatics and Software Engineering Conference (IISEC). IEEE, 2021. С. 1-6.
12. *Shrestha S.* Optimal Traffic Load Balancing Algorithm for Aggregated Ethernet Links on Open vSwitch Platform. 2021.
13. *Ulbricht M. et al.* *Precise fruits*: Hardware supported time-synchronisation on the RaspberryPI //2021 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE, 2021. С. 1-6.
14. *Ulbricht M. et al.* *Emulation vs. Reality*: Hardware/Software Co-Design in Emulated and Real Time-sensitive Networks //European Wireless 2021; 26th European Wireless Conference. VDE, 2021. С. 1-7.
15. *Уймин, А. Г.* Сетевое и системное администрирование. Демонстрационный экзамен КОД 1.1 : учебно-методическое пособие для СПО / А. Г. Уймин. 3-е издание, стереотипное. Санкт-Петербург : Издательство "Лань", 2022. 480 с. ISBN 978-5-8114-9255-8.
16. *Уймин, А. Г.* Периферийные устройства ЭВМ : практикум / А. Г. Уймин. Москва : Ай Пи Ар Медиа, 2023. 429 с. ISBN 978-5-4497-2079-5.
17. *Mishra P., Verma I., Gupta S.* KVMInspector: KVM Based introspection approach to detect malware in cloud environment //Journal of Information Security and Applications. 2020. Т. 51. С. 102460.
18. *Dorđević B. et al.* Performance modeling of file system pairs in hypervisor-based virtual environment applied on KVM hypervisor case study //Journal of Computer and Forensic Sciences. 2022. Т. 1. №. 1. С. 55-75.
19. *Fatahi M. et al.* Open Source Routers: A Survey //arXiv preprint arXiv:2203.01701. 2022.
20. *Греков, В. С.* Перспективы кибербезопасности в нефтегазовой отрасли / *В. С. Греков, А. Г. Уймин* // Губкинский университет в решении вопросов нефтегазовой отрасли России : Тезисы докладов VI Региональной научно-технической конференции, посвященной 100-летию М.М. Ивановой, Москва, 19–21 сентября 2022 года. Москва: Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, 2022. С. 1108-1109.

MODELING A TELECOMMUNICATION NETWORK WITH LINUX NETWORK TOOLS: DIGITAL TWIN TOOLS

ANTON G. UYMIN

Senior lecturer, Gubkin Russian State University of Oil and Gas, Moscow, au-mail@ya.ru

OLEG R. NIKITIN

Doctor in Philosophy, professor, Vladimir State University named after Alexander G. and Nikolay G. Stoletov (Vladimir State University), Vladimir, rtrs@vlsu.ru

ABSTRACT

Introduction: A telecommunications network is a complex system that includes data nodes and a stack of network protocols. The source of traffic is network traffic. As a rule, when designing, upgrading and testing such systems, the most acute problem is the lack of failures in the business process of the enterprise. This problem is solved through two main technologies: emulation and virtual infrastructure. KVM has become the standard for virtualization solutions in telecommunications networks. In particular, solutions based on Linux servers and services (OVS, FRR) have become the de facto standard in solving the problems of virtualization of networks. The main purpose of the study is to analyze the main Linux tools for creating a digital twin of a telecommunication network. Considered Digital Twin as a virtual model of a real telecommunications network, which allows you to accurately represent all of its components and structure. The considered tools can be used both separately and jointly to solve the main tasks of modeling a digital twin. The load on the network was obtained during the processing of network data within the digital twin of the telecommunications network. In this case, the load on the central processor should be taken into account when simulating processes similar to the real network. The development was implemented as part of the High-Tech Championship 2022.

Keywords: telecom network twin; network; virtual; infrastructure; modeling.

REFERENCES

1. Methods of ensuring the stability of the protection system of information and telecommunications network as a dynamic managed system. M. Karpov, M. Kotsinyak, A. Nechepurenko, R. Perov. State and prospects of modern science in the direction of "Information Security" : Proceedings of the III All-Russian Scientific and Technical Conference, Anapa, 21-22 April 2021. Anapa: Federal State Autonomous Institution "Military Innovation Technopolis "ERA", 2021. Pp. 690-696.
2. Shi J. et al. Optimization and decomposition methods in network traffic prediction models: A review and discussion. IEEE Access. 2020. VOL. 8. Pp. 202858-202871.
3. K. A. Grishchenko et al. A computer model of a telecommunication network of modular type, base on digital double construction. Actual Problems of Info-Telecommunications in Science and Education. 2021. Pp. 53-58.
4. Shkarupeta E. V., Kolesnikova V. B., Belyantseva O. M. Metavselenium as a spatial digital double in Industry 5.0. 2021. Pp. 96-116.
5. Makhmudov R. T. Analysis of encrypted network traffic using machine learning. R. T. Makhmudov, A. G. Uimin. Gubkin University in addressing issues of oil and gas industry in Russia : Abstracts of VI Regional Scientific and Technical Conference dedicated to the 100th anniversary of M.M. Ivanova, Moscow, 19-21 September 2022. Moscow: Gubkin Russian State University of Oil and Gas (National Research University), 2022. Pp. 1133-1134.
6. Vyugov S. G., Kozlov S. V. Analysis of characteristics and possibilities of virtual network namespace spaces in the operating system gnu/linux. Actual Problems of Info-telecommunication in Science and Education (APINO 2022). 2022. Pp. 315-319.
7. Jain S. M., Jain S. M. Namespaces. Linux Containers and Virtualization: A Kernel Perspective. 2020. Pp. 31-43.
8. Lackorzynski T., Köpsell S., Strufe T. A comparative study on virtual private networks for future industrial communication systems. 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS). IEEE, 2019. Pp. 1-8.
9. Pandi S. et al. Networking tools. Computing in Communication Networks. Academic Press, 2020. Pp. 431-456.
10. Rai S. S., Monis L., Tahiliani M. P. NeST: Network Stack Tester. Proceedings of the Applied Networking Research Workshop. 2020. Pp. 32-37.
11. Bazai S. U. et al. Kernel virtual machine based high performance environment for grid and jungle computing. 2021 2nd International Informatics and Software Engineering Conference (IISEC). IEEE, 2021. Pp. 1-6.
12. Shrestha S. Optimal Traffic Load Balancing Algorithm for Aggregated Ethernet Links on Open vSwitch Platform. 2021.
13. Ulbricht M. et al. Precise fruits: Hardware supported time-synchronisation on the RaspberryPI . 2021 International Conference on Smart Applications, Communications and Networking (SmartNets). IEEE, 2021. Pp. 1-6.
14. Ulbricht M. et al. Emulation vs. Reality: Hardware/Software Co-Design in Emulated and Real Time-sensitive Networks. European Wireless 2021; 26th European Wireless Conference. VDE, 2021. Pp. 1-7.
15. Uimin, A. G. Network and System Administration. Demonstration exam KOD 1.1 : educational and methodical manual for SPO. 3rd edition, stereotyped. Saint-Petersburg : Lan' Publisher, 2022. 480 p.
16. Uimin, A. G. Peripheral computer devices : a practical course. Moscow : A.P. Ar Media, 2023. 429 p.
17. Mishra P., Verma I., Gupta S. KVMInspector: KVM Based introspection approach to detect malware in cloud environment. Journal of Information Security and Applications. 2020. T. 51. P. 102460.
18. Đorđević B. et al. Performance modeling of file system pairs in hypervisor-based virtual environments applied on KVM hypervisor case study. Journal of Computer and Forensic Sciences. 2022. T. 1. №. 1. Pp. 55-75.
19. Fatahi M. et al. Open Source Routers: A Survey. arXiv preprint arXiv:2203.01701. 2022.
20. Grekov, V. S. Prospects of cybersecurity in the oil and gas industry. V. S. Grekov, A. G. Uimin. Gubkin University in dealing with oil and gas industry in Russia : Abstracts of the VI Regional Scientific and Technical Conference dedicated to the 100th anniversary of M.M. Ivanova, Moscow, 19-21 September 2022. Moscow: Gubkin Russian State University of Oil and Gas (National Research University), 2022. Pp. 1108-1109.