|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  Федеральное государственное автономное образовательное учреждение высшего образования  «Санкт-Петербургский государственный университет аэрокосмического приборостроения»  ФАКУЛЬТЕТ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  КУРСОВОЙ ПРОЕКТ  ЗАЩИЩЕН С ОЦЕНКОЙ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  РУКОВОДИТЕЛЬ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | преподаватель |  |  |  | И.Д. Попов | | должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |  |  | | --- | | ПОЯСНИТЕЛЬНАЯ ЗАПИСКА  К КУРСОВОМУ ПРОЕКТУ | | Проектирование компьютерной сети АЗС |   по дисциплине: МДК 01.02 Организация, принципы построения и функционирования компьютерных сетей |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | С142 |  |  |  | В.И. Тихонов |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2024

СОДЕРЖАНИЕ

Изм.

Лист

№ докум.

Подп.

Дата

Лист

4

КП.09.02.06.21ПЗ

Разраб.

Тихонов В.И.

Пров.

Попов И.Д.

Н. контр.

Утв.

Проектирование компьютерной сети АЗС

Пояснительная записка

Лит.

Листов

ФСПО ГУАП

[ВВЕДЕНИЕ 5](#_Toc167142136)

[1 Теоретическая часть 6](#_Toc167142137)

[1.1 Описание предметной области 6](#_Toc167142138)

[1.2 Принципы построения компьютерных сетей 6](#_Toc167142139)

[1.3 Постановка задачи 7](#_Toc167142140)

[2 Практическая часть 9](#_Toc167142141)

[2.1 Выбор сетевого оборудования и его обоснование 9](#_Toc167142142)

[2.2 Базовая настройка сети 10](#_Toc167142143)

[2.3 Настройка маршрутизации 13](#_Toc167142144)

[2.4 Настройка сервисов 16](#_Toc167142145)

[2.5 Тестирование работоспособности сети 18](#_Toc167142146)

[ЗАКЛЮЧЕНИЕ 23](#_Toc167142147)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 24](#_Toc167142148)

[ПРИЛОЖЕНИЕ А 25](#_Toc167142149)

[ПРИЛОЖЕНИЕ Б 26](#_Toc167142150)

[ПРИЛОЖЕНИЕ В 27](#_Toc167142151)

[ПРИЛОЖЕНИЕ Г 28](#_Toc167142152)

# ВВЕДЕНИЕ

С развитием технологий и автоматизации компьютерные сети становятся неотъемлемой частью инфраструктуры различных предприятий и организаций. В рамках данного курсового проекта рассматривается проектирование компьютерной сети для автозаправочной станции (АЗС), что представляет собой важную задачу в условиях современной торговли и сервиса.

В первой части работы проводится обзор предметной области, включающий описание особенностей функционирования АЗС и их специфических потребностей в сетевой инфраструктуре. Также рассматриваются основные принципы построения компьютерных сетей, которые являются основой для дальнейшего проектирования и настройки сети для АЗС.

Во второй части проекта представлены конкретные этапы проектирования и настройки сети. Включая выбор необходимого сетевого оборудования с обоснованием выбора, базовую настройку сети, конфигурацию маршрутизации и настройку сервисов, необходимых для обеспечения работоспособности и безопасности сети АЗС. Также проводится тестирование работоспособности сети, что позволяет убедиться в корректности ее функционирования и готовности к использованию.

Целью данного проекта является создание надежной и эффективной сетевой инфраструктуры для АЗС, способной обеспечить бесперебойную работу оборудования, безопасность передаваемых данных и удобство управления всей сетью.

# 1 Теоретическая часть

## 1.1 Описание предметной области

В контексте предоставленных требований автозаправочная станция должна быть оборудована компьютерной сетью, поддерживающей российские операционные системы как на клиентских, так и на серверных устройствах. Сеть должна осуществлять поддержку IPv4, автоматическую конфигурацию сетевых настроек узлов и обеспечивать доступ к устройствам по доменным именам.

Для обеспечения безопасности и контроля доступа, сеть должна иметь межсетевой экран (firewall) и использовать механизм Network Address Translation (NAT) для доступа в Интернет. Важным аспектом является организация доступа к серверу с базой данных и веб-серверу, размещенным в главном офисе, при этом доступ к базе данных должен быть ограничен только из внутренней сети, а доступ в Интернет должен осуществляться через главный офис.

Кроме того, учитывая распределенную природу бизнеса, несколько филиалов должны быть связаны с главным офисом через виртуальную персональную сеть (VPN), обеспечивая обмен данными и централизованное управление. Для обеспечения доступа к веб-серверу, в главном офисе используется обратный прокси-сервер на базе nginx, что повышает безопасность и эффективность работы сети.

## 1.2 Принципы построения компьютерных сетей

Построение компьютерных сетей для автозаправочных станций основывается на ряде ключевых принципов, обеспечивающих надежность, безопасность и эффективность функционирования всей инфраструктуры. Ниже перечислены основные принципы, которые следует учитывать при проектировании сети для АЗС:

1. Контроль доступа и безопасность: важным аспектом является обеспечение безопасности сети и контроля доступа к ресурсам. Это включает в себя использование механизмов аутентификации и авторизации, настройку межсетевого экрана (firewall) для фильтрации трафика.
2. Управление сетью: для эффективного управления сетью необходимо использовать инструменты мониторинга, управления и конфигурации. Это включает в себя системы мониторинга состояния сети, системы резервного копирования и восстановления, а также средства автоматизации конфигурации сетевого оборудования.
3. Масштабируемость и гибкость: при проектировании сети необходимо учитывать возможность масштабирования и гибкости, чтобы обеспечить ее адаптацию к изменяющимся потребностям бизнеса. Это включает в себя выбор гибкого и масштабируемого сетевого оборудования, а также использование стандартных протоколов и технологий, позволяющих легко внедрять изменения и расширять функциональность сети.
4. Оптимизация производительности: для обеспечения высокой производительности сети необходимо учитывать оптимизацию трафика и ресурсов. Это включает в себя правильное размещение серверов и другого сетевого оборудования, использование качественных сетевых кабелей и активных устройств, а также оптимизацию конфигурации сетевых протоколов и сервисов.

## 1.3 Постановка задачи

Целью данного проекта является проектирование компьютерной сети для автозаправочной станции (АЗС) с учетом предоставленных требований и особенностей предметной области. Основной задачей проекта является создание надежной, безопасной и эффективной сетевой инфраструктуры, способной обеспечить бесперебойное функционирование всех систем АЗС, а также обеспечить доступ к важным сервисам и ресурсам как внутри сети, так и из внешней сети.

Ключевые задачи проекта включают в себя:

1. Настройка сетевого оборудования, включая маршрутизаторы, коммутаторы и межсетевой экран (firewall), с учетом требований безопасности и доступности.
2. Конфигурация DHCP-сервера для автоматической выдачи IP-адресов и других сетевых параметров клиентским устройствам.
3. Настройка DNS-сервера для обеспечения доступа к устройствам по доменным именам и решения имен внутри сети.
4. Реализация механизма NAT для обеспечения доступа в Интернет и скрытия внутренних IP-адресов от внешней сети.
5. Настройка GRE-туннеля для обеспечения удаленного доступа к сети АЗС для сотрудников и администраторов.
6. Развертывание веб-сервера Apache2, обратного прокси сервера nginx и SQL-сервера с ограничением доступа из внешней сети и обеспечением доступа из внутренней сети.
7. Тестирование работоспособности и безопасности сети, включая проверку корректности настроек, обнаружение и устранение возможных проблем и анализ производительности сети.

В конечном итоге выполнение этих задач должно привести к созданию сетевой инфраструктуры, которая удовлетворяет всем требованиям безопасности, надежности и эффективности, а также обеспечивает комфортный и безопасный доступ к сервисам и ресурсам как внутри, так и вне сети АЗС.

# 2 Практическая часть

## 2.1 Выбор сетевого оборудования и его обоснование

Выбор сетевого оборудования является важным этапом проектирования компьютерной сети для автозаправочной станции (АЗС). В данном разделе будут рассмотрены критерии выбора сетевого оборудования и обоснование выбранных решений, учитывая требования безопасности, надежности и эффективности функционирования сети.

В качестве сетевого оборудования для главного офиса был выбран маршрутизатор MikroTik RB5009UPR+S+IN. Оборудование Mikrotik было выбрано по нескольким причинам, таким как: наличие необходимых технологий, таких как GRE, DHCP, DNS, NAT; доступности в России; удобному графическому интерфейсу – WinBox и постоянно обновляющийся операционной системе. Эта модель является средне бюджетной, у нее 7 гигабитных портов RJ-45 со скорость, 1 порт cо скоростью передачи данных 2.5 Гбит/с и порт SFP+ для соединений на скорости 10 Гбит/с. Такой скорости передачи данных будет достаточно для устройств в офисе. Для коммутации был выбран коммутатор ZYXEL GS-108B v3, имеющий 8 гигабитных портов Он удовлетворяет требованиям по обеспечению скорости передачи данных. В офисе 4 настольных компьютера и 2 сервера.

В каждый филиал выбраны по 1 маршрутизатору Mikrotik RB2011UiAS-IN — это низкобюджетный маршрутизатор, но тем не менее, подходит под требования скорости передачи и обладает такими же технологиями, как и средне бюджетный маршрутизатор в главном офисе. В качестве коммутаторов в филиалы были выбраны так же ZYXEL GS-108B v3. В филиалах установлены по 3 настольных компьютера.

В качестве среды передачи внутри локальной сети используется кабель витой пары категории 5e в связке с интерфейсом RJ-45. Скорость передачи данных до 1 Гбит/с, как и у портов сетевых устройств. Интерфейс RJ-45 обеспечивает совместимость кабеля и оборудования. Экранирование поможет снизить помехи.

На границе выхода в интернет будет использоваться оптоволоконный кабель, выходящий из SFP+ порта со скорость передачи 10 Гбит/с, чтобы обеспечить доступ в Интернет для всех устройств компании. Проводка кабеля осуществляется провайдером, поэтому его стоимость не включена в траты на сетевое оборудование.

В таблице 1 приведены выбранные сетевые устройства, их количество, цена и общая стоимость.

Таблица 1– Сетевое оборудование

|  |  |  |  |
| --- | --- | --- | --- |
| Название | Цена (руб.) | Количество | Стоимость (руб.) |
| Маршрутизатор MIKROTIK RB5009UPR+S+IN | 49063 | 1 | 49063 |
| Маршрутизатор MIKROTIK RB2011ILS-IN | 15901 | 2 | 31 802 |
| Коммутатор ZYXEL GS-108B v3 | 3 999 | 3 | 11 997 |
| Кабель SkyNet Premium CSP-FTP-4-CU-OUT/100 | 3 340 | 3 | 10 020 |
| Разъем Hyperline RJ-45 PLUG-8P8C-U-C5-100 | 2 264 | 1 | 2 264 |
| Итого: | | | 103 148 |

## 2.2 Базовая настройка сети

После выбора и обоснования сетевого оборудования необходимо перейти к практической реализации проекта. Далее представлены схемы сети и IP-план, которые наглядно демонстрируют организацию сетевой инфраструктуры АЗС. Эти схемы помогут визуализировать расположение оборудования, подключение узлов и распределение IP-адресов, обеспечивая ясное понимание структуры и логики построения сети.

Схема сети L1 показана в приложении А.

Схема сети L2 показана в приложении Б.

Схема сети L3 показана в приложении В.

Схема диаграмм маршрутизации показана в приложении Г.

Таблица 2 – IP-план

|  |  |  |  |
| --- | --- | --- | --- |
| Название устройства | Интерфейс | IP-адрес | DHCP  (да/нет) |
| hq-r1-21 | lo | 21.4.4.4/32 | нет |
| ether1 | 100.21.1.2/28 | да |
| ether2 | 10.21.1.1/24 | нет |
| toR5 | 10.21.45.4/24 | нет |
| toR6 | 10.21.46.4/24 | нет |
| br1-r1-21 | lo | 21.5.5.5/32 | нет |
| ether1 | 100.21.2.2/28 | да |
| ether2 | 10.21.2.1/24 | нет |
| toR4 | 10.21.45.5/24 | нет |
| br2-r1-21 | lo | 21.6.6.6/32 | нет |
| ether1 | 100.21.3.2/28 | да |
| ether2 | 10.21.3.1/24 | нет |
| toR4 | 10.21.46.6/24 | нет |
| hq-srv-sql-21 | ens33 | 10.21.1.3/24 | да |
| hq-srv-proxy-21 | ens33 | 10.21.1.4/24 | да |
| hq-pc1-21 | e0 | 10.21.1.5/24 | да |
| hq-pc2-21 | e0 | 10.21.1.6/24 | да |
| hq-pc3-21 | e0 | 10.21.1.7/24 | да |
| hq-pc4-21 | ens33 | 10.21.1.8/24 | да |
| br1-pc1-21 | ens33 | 10.21.2.3/24 | да |
| br1-pc2-21 | e0 | 10.21.2.4/24 | да |
| br1-pc3-21 | e0 | 10.21.2.5/24 | да |
| br2-pc1-21 | e0 | 10.21.3.3/24 | да |
| br2-pc2-21 | e0 | 10.21.3.4/24 | да |
| br2-pc3-21 | e0 | 10.21.3.5/24 | да |

Настройка любой сети начинается с назначения IP-адреса, в том числе на loopback интерфейс, для удобства доступа к сетевому оборудованию. На рисунке 1 изображены команды, которые назначают IP-адрес на маршрутизаторе.



Рисунок 1 – Назначения IP-адреса на маршрутизаторе

Внешний адрес маршрутизатор получает от провайдера по DHCP. Для этого необходимо включить DHCP-клиент на нужном порту. Процесс включения изображен на рисунке 2.



Рисунок 2 – Включение DHCP-клиента на порту

Устройствам в локальной сети так же необходим адрес. Для удобства и масштабируемости, они будут получать IP-адреса от DHCP-сервера, который находится на маршрутизаторе в офисе [[1]](#_СПИСОК_ИСПОЛЬЗОВАННЫХ_ИСТОЧНИКОВ). На рисунках 3 и 4 изображена настройка DHCP-сервера на маршрутизаторе.



Рисунок 3 – Настройка диапазона адресов для клиентов

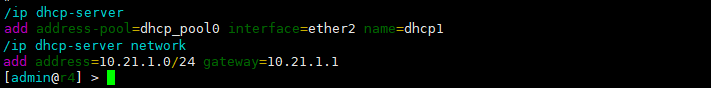


Рисунок 4 – Настройка DHCP-сервера на маршрутизаторе

Также необходимо сделать IP-адреса, выданные по DHCP статическими. Это понадобится для создания DNS-записей. На рисунке 5 изображен процесс привязки IP-адреса к MAC-адресу.

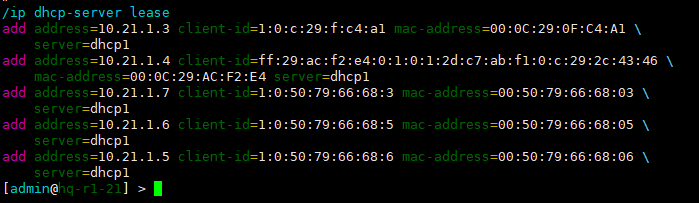


Рисунок 5 – Привязка IP-адреса к MAC-адресу на маршрутизаторе.

Следующим этапом будет настройка PAT (Трансляция порт-адрес) на границе провайдера, для трансляции локальных адресов в глобальный. Настройка PAT изображена на рисунке 6.



Рисунок 6 – Настройка PAT на маршрутизаторе

## 2.3 Настройка маршрутизации

Для начала необходимо настроить GRE-туннели между офисами компании для связности корпоративной сети [[2]](#_СПИСОК_ИСПОЛЬЗОВАННЫХ_ИСТОЧНИКОВ). Настройка туннеля с двух концов изображена на рисунках 7 и 8.



Рисунок 7 – Настройка GRE-туннеля на маршрутизаторе в главном офисе



Рисунок 8 – Настройка GRE-туннеля на маршрутизаторе в филиале

Далее необходимо настроить динамическую маршрутизацию, чтобы маршрутизаторы в офисах знали о локальных сетях друг друга. В данном случае был выбран протокол OSPF, он является наиболее современным и распространённым. Настройка OSPF на двух маршрутизаторах изображена на рисунках 9 и 10.

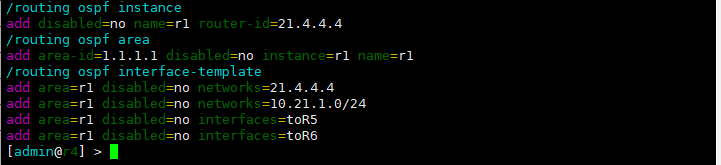


Рисунок 9 – Настройка OSPF на маршрутизаторе в главном офисе

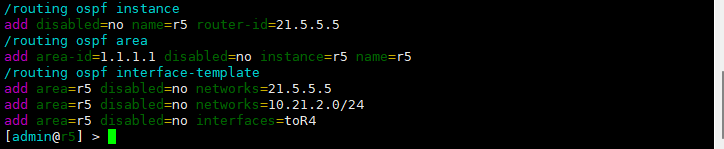


Рисунок 10 – Настройка OSPF на маршрутизаторе в филиале

Трафик в Интернет из филиалов должен проходить через главный офис, для этого на маршрутизаторах в филиалах необходимо в качестве шлюза по умолчанию (default gateway) назначить GRE-туннель и отключить получение шлюза по умолчанию у провайдера. На рисунке 11 изображена настройка, позволяющая отказаться от получения шлюза по умолчанию у провайдера, на 12 рисунке изображено назначение шлюза по умолчанию.



Рисунок 11 – Выключение функции получения шлюза по умолчанию у провайдера на маршрутизаторе



Рисунок 12 – Назначение GRE-туннеля шлюзом по умолчанию на маршрутизаторе в филиале

Устройствам в локальной сети необходимы доменные имена, для удобства обращения к ним, а также возможность обращаться по доменным именам других устройств в локальной сети и веб-серверов в Интернете. Для этих целей был настроен кэширующий DNS-сервер на маршрутизаторе в главном офисе, а в филиалах в качестве DNS-сервера был указан маршрутизатор в главном офисе. Настройка DNS-служб изображена на рисунках 13 и 14.

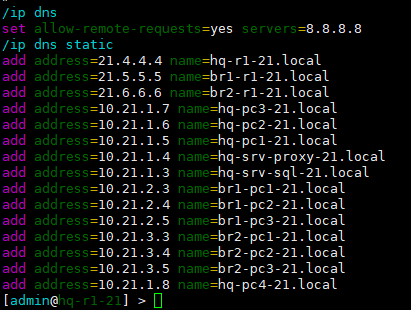


Рисунок 13 – Настройка DNS-сервера на маршрутизаторе в главном офисе



Рисунок 14 – Настройка DNS-сервера на маршрутизаторе в филиале

## 2.4 Настройка сервисов

Предприятию необходим веб-сервер и сервер базы данных. Это было реализовано с помощью технологии контейнеризации, а именно docker-compose на отечественной операционной системе RedOS [[3]](#_СПИСОК_ИСПОЛЬЗОВАННЫХ_ИСТОЧНИКОВ). Веб-сервер был запущен на базе Apache2, а сервер базы данных на базе PostgreSQL. На рисунке 15 изображена информация об операционной системе и содержимое конфигурационного файла «docker-compose.yml» для запуска нескольких контейнеров.



Рисунок 15 – Информация об операционной системе и содержимое конфигурационного файла «docker-compose.yml»

Для обеспечения безопасности, доступ к веб-серверу был организован через обратный прокси сервер на базе nginx на операционной системе Debian [[4]](#_СПИСОК_ИСПОЛЬЗОВАННЫХ_ИСТОЧНИКОВ). На рисунке 16 представлено содержимое конфигурационного файла «reverse-proxy».



Рисунок 16 – Содержимое конфигурационного файла «reverse-proxy»

Необходимо, чтобы прокси сервер был доступен из Интернета, для этого необходимо настроить проброс на 80 порт. На рисунке 17 изображена настройка проброса портов.



Рисунок 17 – Проброс 80 порта на маршрутизаторе

Управление сетевым оборудованием, доступно по протоколу telnet, а серверами по SSH. В обоих случаях необходимо знать имя пользователя и пароль. Для обеспечения безопасности на серверах запрещено подключаться с пользователя «root», эта настройка продемонстрирована на рисунке 18.

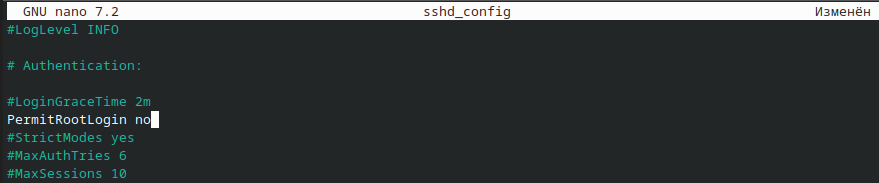


Рисунок 18 – Запрет подключаться с пользователя «root» по SSH на сервере

## 2.5 Тестирование работоспособности сети

Для начала нужно получить IP-адрес на ПК по DHCP и таким образом проверить работоспособность DHCP-сервера. Процесс получения IP-адреса по DHCP изображен на рисунке 19.

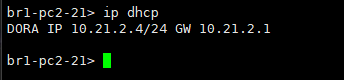


Рисунок 19 – Получения IP-адреса по DHCP на ПК

Далее отследить трафик, выполнив трассировку маршрута на ПК из филиала, указав доменное имя ПК в главном офисе как адрес назначения. Таким образом можно проверить работоспособность GRE-туннеля, динамической маршрутизации и DNS-сервера сразу. На рисунке 20 изображена трассировка маршрута на локальное доменное имя.

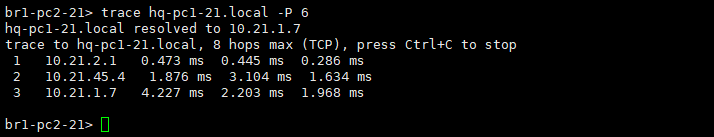


Рисунок 20 – Трассировка маршрута на доменное имя ПК в главном офисе

Также на рисунке 21 изображены маршруты, полученные по протоколу OSPF.

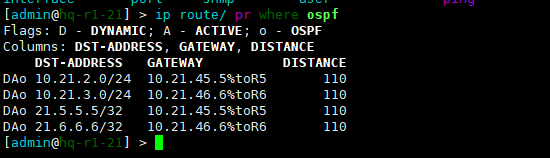


Рисунок 21 – OSPF маршруты на маршрутизаторе

Таким же образом можно проверить доступ в интернет и работу NAT, если указать внешнее доменной имя, как адрес назначения. На рисунке 22 изображена трассировка маршрута на глобальное доменное имя и icmp-запрос на то же имя.

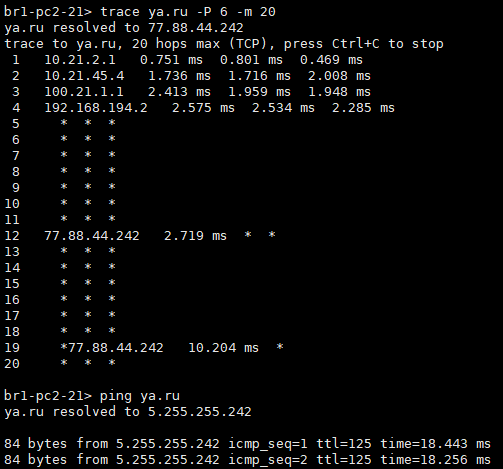


Рисунок 22 – Trace и ping доменного имени «ya.ru»

Так же на рисунке 23 изображен мониторинг трафика на границе выхода в Интернет, где видно, что IP-адрес ПК подменился на IP-адрес интерфейса маршрутизатора.

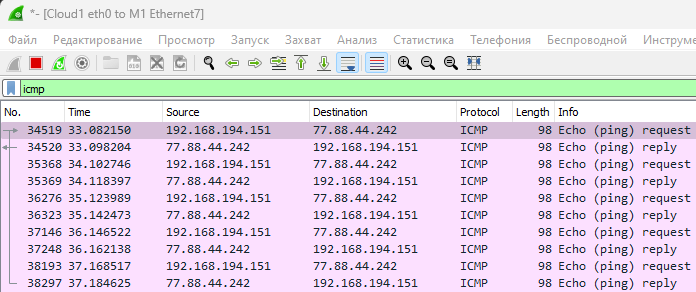


Рисунок 23 – Мониторинг трафика в Wireshark

На рисунках 24 и 25 продемонстрирована работа протоколов удаленного доступа.

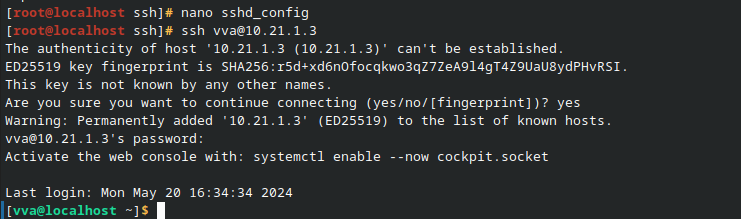


Рисунок 24 – Подключения по SSH к серверу

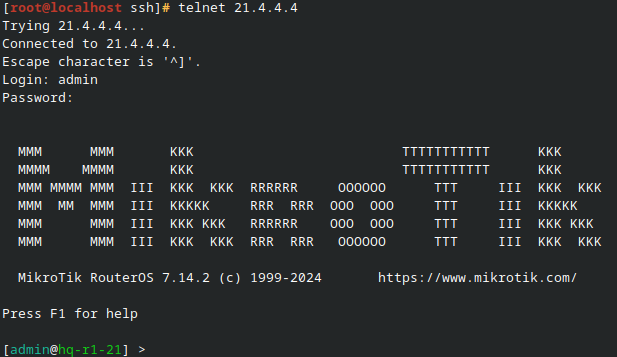


Рисунок 25 – Подключения по telnet к маршрутизатору

Последним этапом будет проверка доступности серверов. Для начала можно подключиться к серверу базы данных, используя графический клиент «DBeaver» и создать схему «tikhonov» для проверки работоспособности. Интерфейс клиента баз данных изображен на рисунке 26.

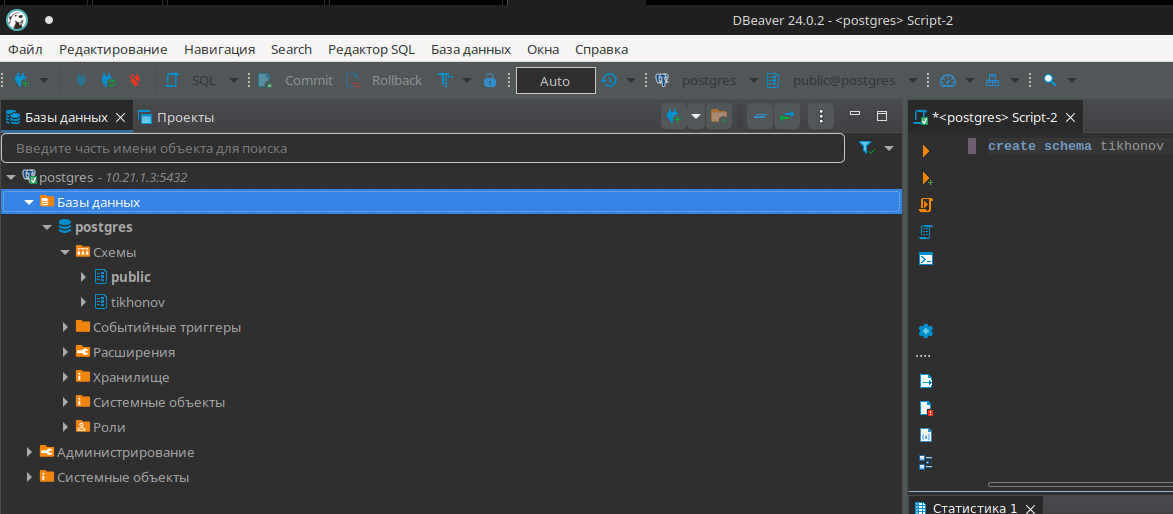


Рисунок 26 – Подключение к серверу базы данных с клиента

Далее необходимо проверить работоспособность обратного прокси сервера, который перенаправляет трафик на веб-сервер. Для этого нужно вписать IP-адрес интерфейса маршрутизатора, на котором настроен проброс портов, в браузер. Процесс открытия веб-страницы изображен на рисунке 27.

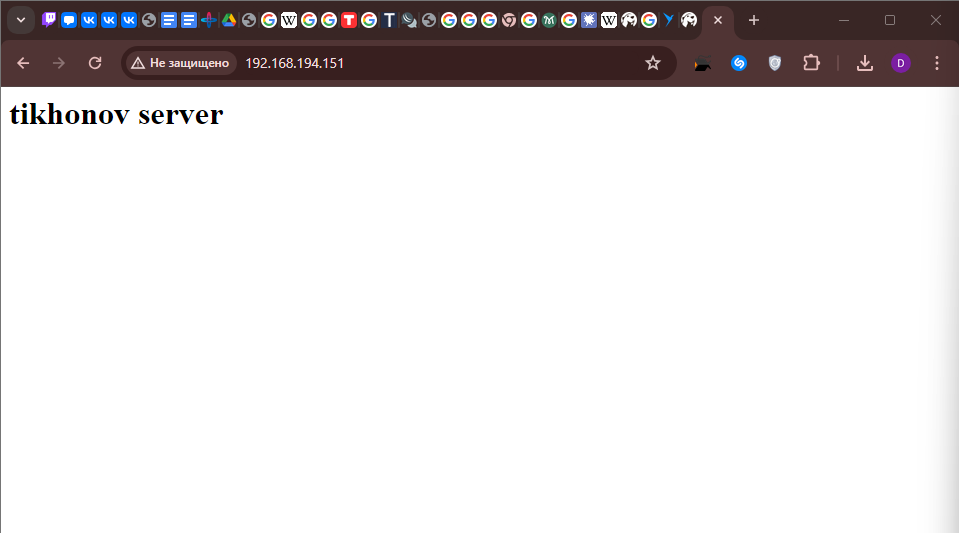


Рисунок 27 – Открытие веб-страницы из внешней сети

# ЗАКЛЮЧЕНИЕ

В ходе выполнения данного курсового проекта была разработана и спроектирована компьютерная сеть для автозаправочной станции (АЗС), учитывающая все необходимые требования и особенности предметной области.

В теоретической части были рассмотрены основные принципы построения компьютерных сетей, включая автоматизацию настройки сети с помощью DHCP, обеспечение удобного доступа к устройствам через DNS, использование NAT для защиты сети и обеспечение доступа в Интернет, а также применение VPN для безопасного удаленного доступа и настройку веб- и SQL-серверов для внутреннего использования.

Практическая часть проекта включала выбор и обоснование сетевого оборудования, настройку сети, маршрутизацию, настройку необходимых сервисов и тестирование работоспособности сети. Разработанные схемы сети и IP-план наглядно продемонстрировали организацию сетевой инфраструктуры АЗС, распределение IP-адресов и подключение узлов.

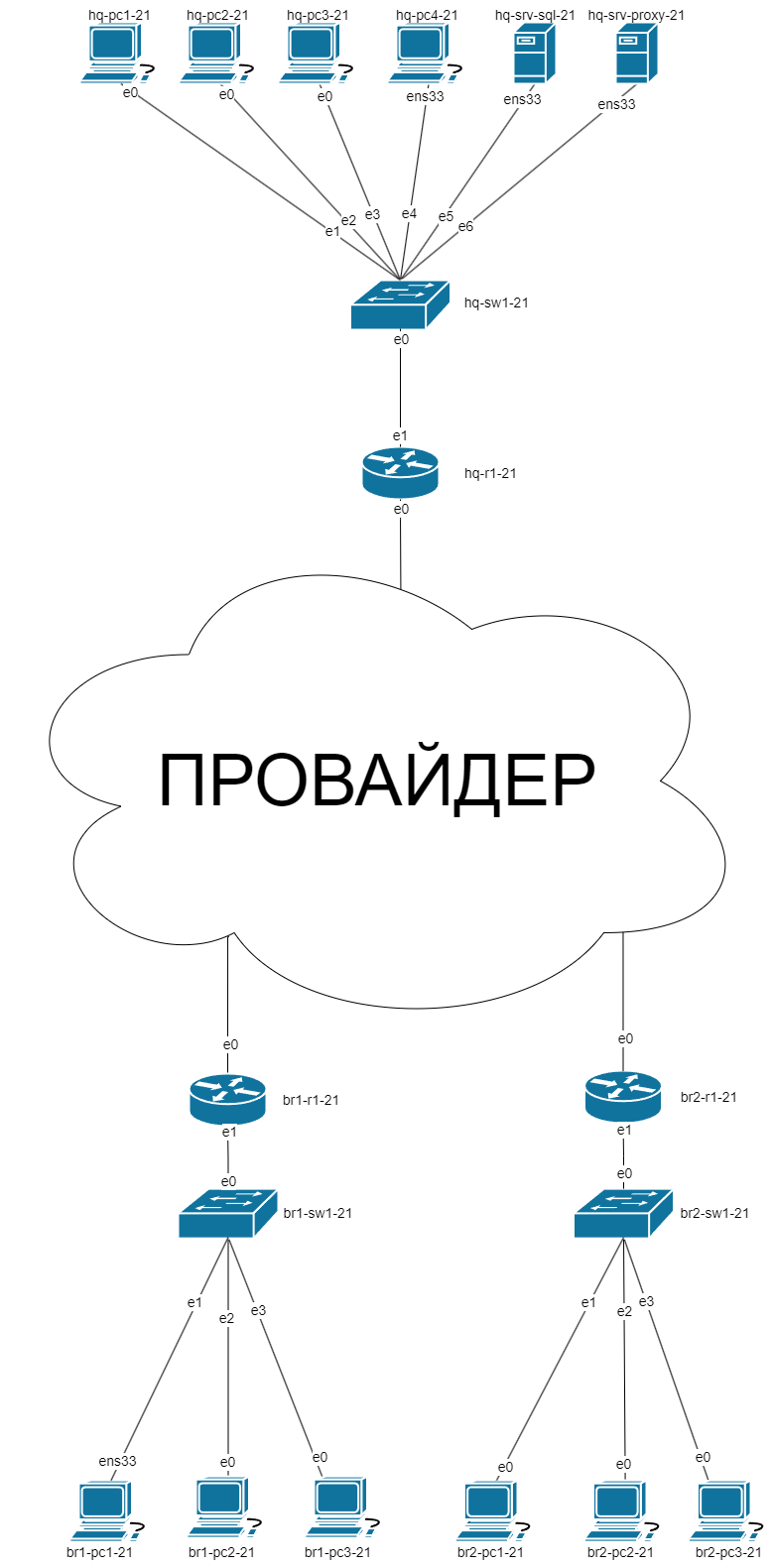
Результаты тестирования подтвердили корректность настроек и готовность сети к эксплуатации, обеспечивая надежную, безопасную и эффективную работу всех систем автозаправочной станции. Таким образом, поставленные задачи были успешно выполнены, что свидетельствует о достижении целей проекта и готовности сети к практическому использованию.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. RouterOS - MikroTik Documentation — URL: <https://help.mikrotik.com/docs/display/ROS/RouterOS> (дата обращения: 13.05.2024)
2. RouterOS Documentation. – URL: <https://wiki.mikrotik.com/wiki/Manual:TOC> (дата обращения: 14.05.2024)
3. Руководство - База знаний РЕД ОС. — URL: <https://redos.red-soft.ru/base/manual/> (дата обращения: 15.05.2024)
4. Nginx Reverse Proxy. — URL: <https://docs.nginx.com/nginx/admin-guide/web-server/reverse-proxy/> (дата обращения: 16.05.2024)

# ПРИЛОЖЕНИЕ А

**Схема сети L1**



# ПРИЛОЖЕНИЕ Б

**Схема сети L2**



# ПРИЛОЖЕНИЕ В

**Схема сети L3**



# ПРИЛОЖЕНИЕ Г

**Диаграмма маршрутизации**

