МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 42

КУРСОВАЯ РАБОТА
ЗАЩИЩЕНА С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ

канд. техн. наук , доцент		В. М. Смирнов
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К КУРСОВОЙ РАБОТЕ

СОЗДАНИЕ МОДЕЛИ СЕТИ НА СТЕНДЕ ПО ЗАДАННОЙ ТОПОЛОГИИ

по дисциплине:

ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ гр. №	4326		Г. С. Томчук
		подпись, дата	инициалы, фамилия

Санкт-Петербург 2025

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И СПЕЦИАЛЬНЫХ ТЕРИМНОВ

- DHCP (Dynamic Host Configuration Protocol) — протокол автоматической настройки, который позволяет сетевым устройствам (компьютерам, телефонам, принтерам) автоматически получать IP-адреса и другие необходимые сетевые параметры (маску подсети, шлюз, DNS-сервер) от DHCP-сервера, избавляя администраторов от ручной настройки и предотвращая конфликты адресов.
- NAT (Network Address Translation) — технология в сетях TCP/IP, которая преобразует (маскирует) частные (локальные) IP-адреса устройств в один публичный (внешний) IP-адрес, позволяя множеству устройств в домашней или офисной сети одновременно выходить в Интернет, экономить IP-адреса и повышать безопасность, скрывая внутреннюю структуру сети.
- VLAN (Virtual Local Area Network) — технология, которая позволяет логически разделить одну физическую сеть на несколько независимых виртуальных сетей (VLAN) для изоляции трафика, повышения безопасности и управляемости, не меняя физическую топологию.
- VPCS (Virtual PC Simulator) — это легкий эмулятор виртуальных компьютеров/хостов, который позволяет быстро создавать узлы в топологиях для тестирования сетевых протоколов, скриптов и команд, предоставляя интерфейс командной строки, похожий на Cisco IOS, но с упрощенным функционалом, чтобы не загружать ресурсы, как полноценная ОС, но имитировать работу хоста.
- VTP (VLAN Trunking Protocol) — проприетарный протокол компании Cisco, используемый в локальных сетях для автоматической синхронизации информации о VLAN (виртуальных локальных сетях) между коммутаторами, что упрощает управление сетью, позволяя создавать и удалять VLAN централизованно, а не на каждом устройстве по отдельности.

ВВЕДЕНИЕ

Современные компьютерные сети являются основой функционирования информационных систем и сервисов, поэтому навыки их проектирования, настройки и анализа имеют ключевое значение для специалистов в области информационных технологий. Моделирование сетей в виртуальных средах позволяет воспроизвести работу реальной инфраструктуры, отработать различные сценарии взаимодействия оборудования и получить практический опыт без необходимости использования физического стенда.

Данная курсовая работа посвящена созданию модели компьютерной сети на стенде по заданной топологии. В процессе выполнения работы используется виртуальная среда EVE-NG, а также сетевое оборудование Cisco и Mikrotik. Особое внимание уделяется настройке коммутации, маршрутизации, разделению сети на VLAN, а также обеспечению корректного взаимодействия между узлами как внутри одного VLAN, так и между различными VLAN.

Целью работы является построение и настройка модели сети, обеспечивающей связность всех компонентов согласно заданной топологии, а также проверка доступа к сети Интернет. Для достижения поставленной цели выполняется подбор характеристик оборудования, реализация карты сети, настройка коммутаторов и маршрутизаторов, а также тестирование работоспособности сети с использованием виртуальных конечных устройств.

1 Техническое задание

Цель выполнения работы — создать модель сети на стенде по заданной топологии.

Работа должна содержать скриншоты с настройкой всех компонентов, доказательства наличия связи компонентов внутри одного VLAN, между разными VLAN и интернетом.

Вариант задания: 17 (7). На рисунке 1 изображена заданная топология сети по варианту.

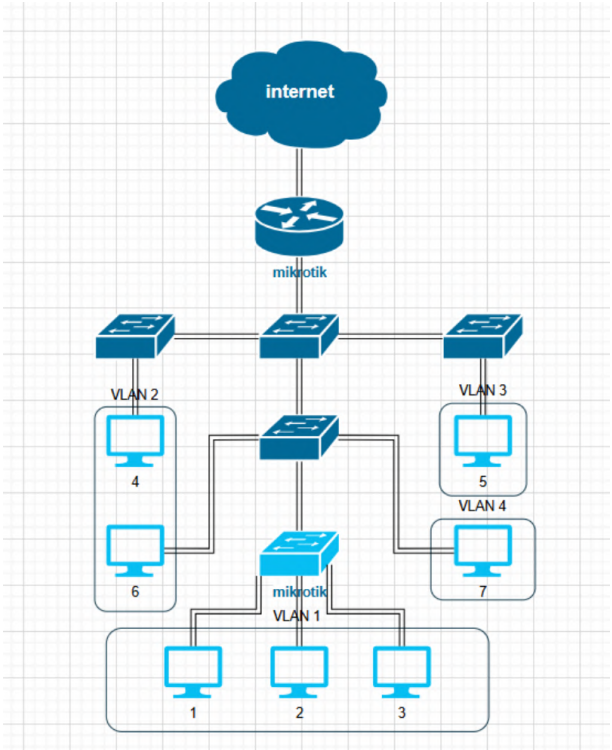

Рисунок 1 — Топология сети (вариант 7)

2 Ход выполнения работы

2.1 Определение характеристик оборудования

Для построения сети на стенде были выбраны следующие сетевые компоненты с указанными характеристиками:

- Cisco IOL Switch (образ «L2-ADVENTERPRISE-M-15.1-20140814»); RAM: 512 MB, Ethernet portGroup: 2. Количество: 4 шт.;
- Mikrotik (образ «mikrotik-6.49.19»); RAM: 256 MB, QEMU Nic: e1000. Количество: 2 шт.;
- Virtual PC (VPCS). Количество: 7 шт.

2.2 Реализация карты сети на стенде

Первым делом была составлена и запущена топологическая модель сети на стенде: узлы расположены согласно схеме и соединены между собой (рисунок 2).

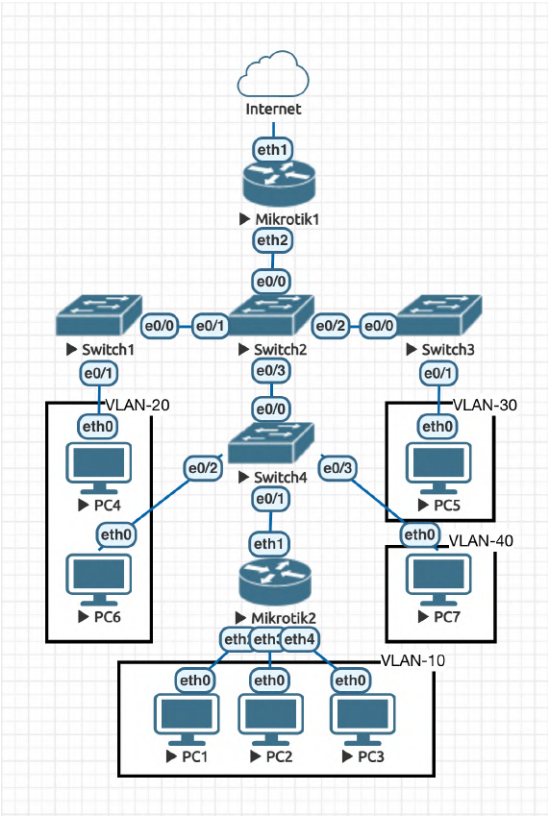

Рисунок 2 — Составленная модель сети

2.3 Настройка коммутаторов Cisco IOL Switch

Далее была произведена настройка коммутаторов Cisco IOL Switch.

В роли VTP-сервера сети был выбран коммутатор Switch2 из-за своего центрального связующего положения в топологии. Сперва необходимо вручную определить все VLAN в создаваемой сети (рисунки 3–4).

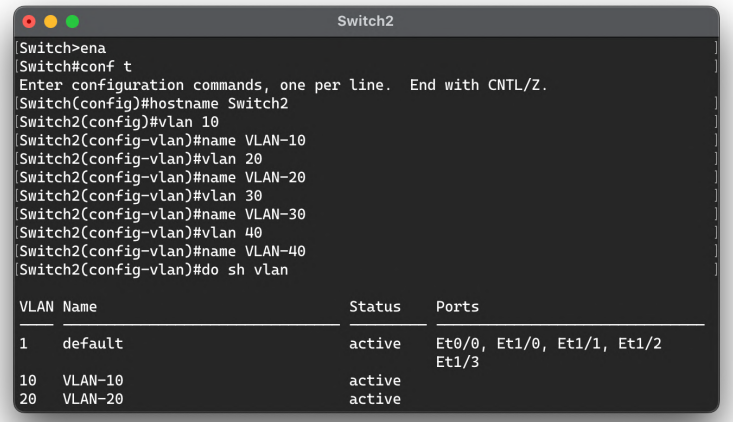

Рисунок 3 — Добавление VLAN на Switch2

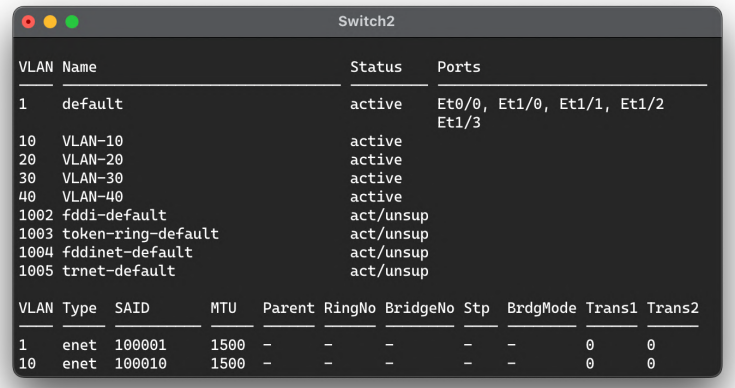

Рисунок 4 — Вывод конфигурации VLAN на Switch2

Затем необходимо настроить порты коммутатора: подписать подключенные к портам устройства, указать режим порта (trunk или access), и для тегируемого trunk-режима отключить автотегирование с помощью команды «switchport trunk encapsulation dot1q», в то время как для режима доступа (access) — присвоить порту соответствующий VLAN с помощью команды «switchport access vlan ID» (рисунки 5–6).

Рисунок 5 — Настройка портов на Switch2

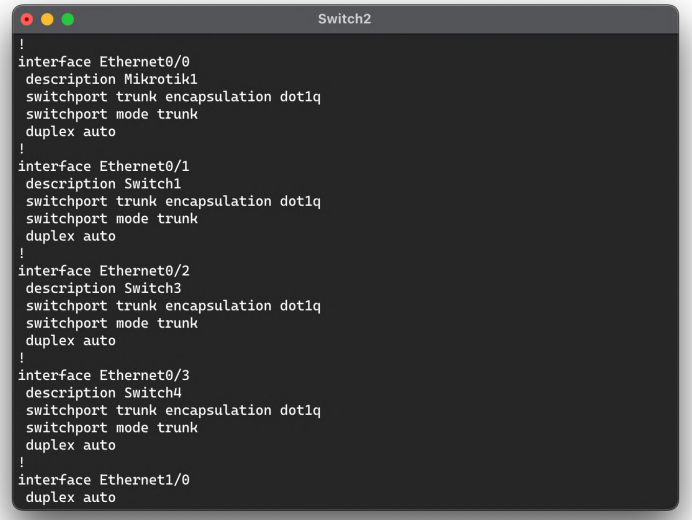

Рисунок 6 — Вывод конфигурации портов на Switch2

После этого можно приступить к настройке VTP-сервера на коммутаторе (рисунки 7–8). После присвоения VTP-серверу режима Primary, нужно настроить VTP-клиенты на всех остальных коммутаторах Cisco (рисунки 9–11).

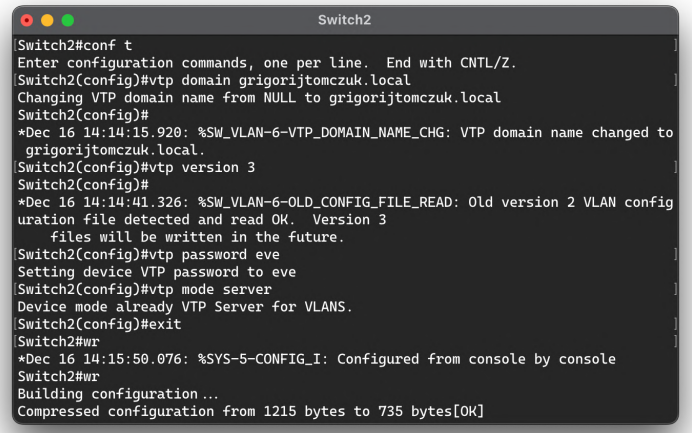

Рисунок 7 — Настройка VTP-сервера на Switch2

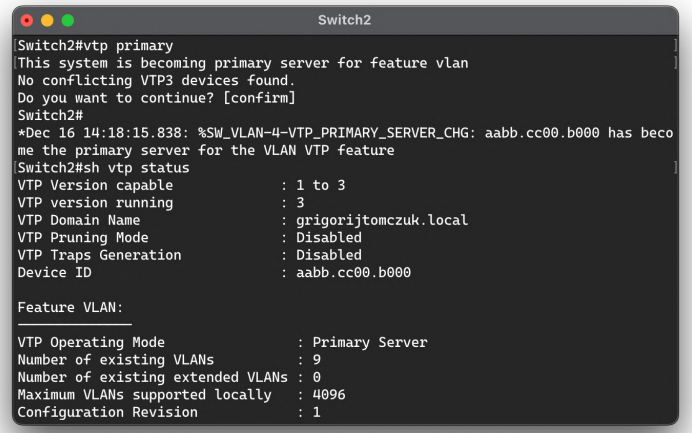

Рисунок 8 — Вывод конфигурации VTP-сервера на Switch2

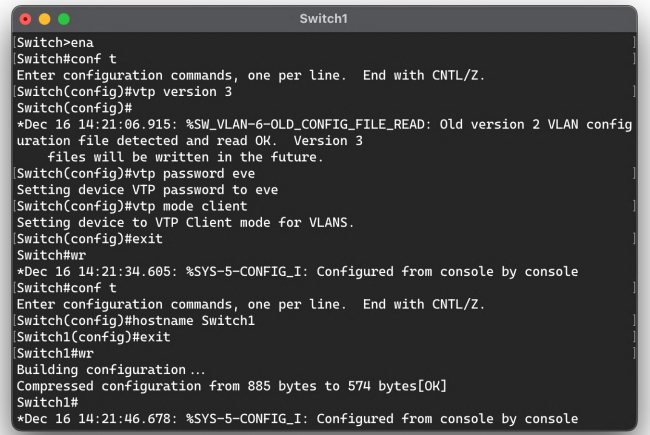

Рисунок 9 — Настройка VTP-клиента на Switch1

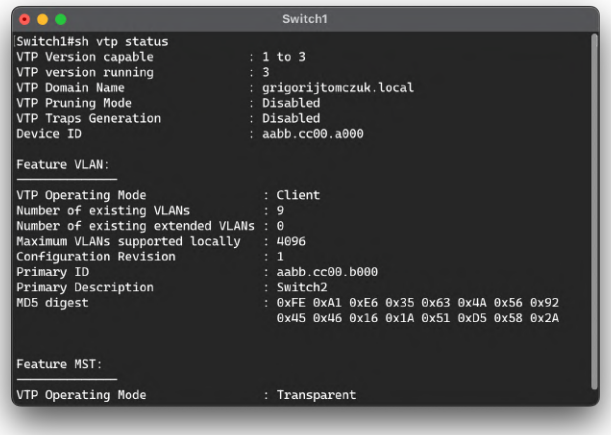

Рисунок 10 — Вывод конфигурации VTP-клиента на Switch1

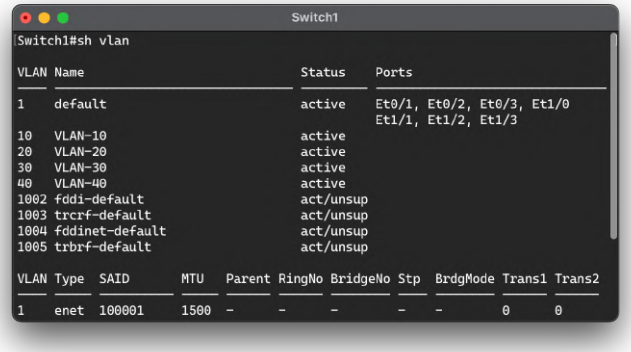

Рисунок 11 — Вывод конфигурации VLAN на Switch1 (VTP-клиент)

Как видно на рисунке 11, VTP-клиент успешно обнаружил созданные ранее VLAN. Аналогичным образом VTP-клиенты были настроены на коммутаторах Switch3 и Switch4. Теперь, когда все коммутаторы «знают» о всех существующих VLAN, необходимо настроить порты коммутаторов, подключенных непосредственно к VPCS (рисунки 12–13).

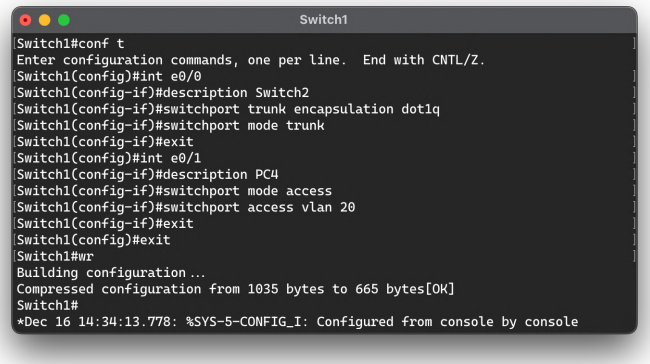

Рисунок 12 — Настройка портов на Switch1

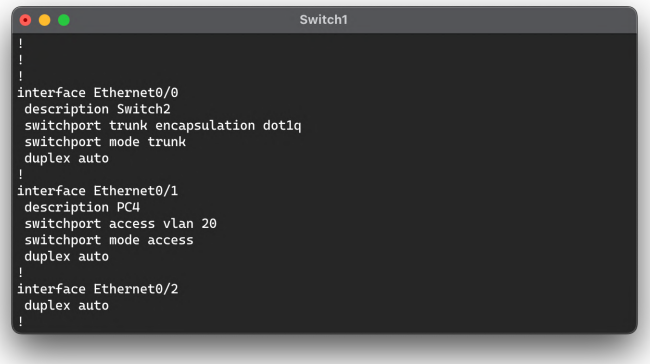

Рисунок 13 — Вывод конфигурации портов на Switch1

Аналогичным образом были настроены порты на коммутаторах Switch3 и Switch4. На рисунках 14–15 представлена конфигурация портов и VLAN на коммутаторе Switch4.

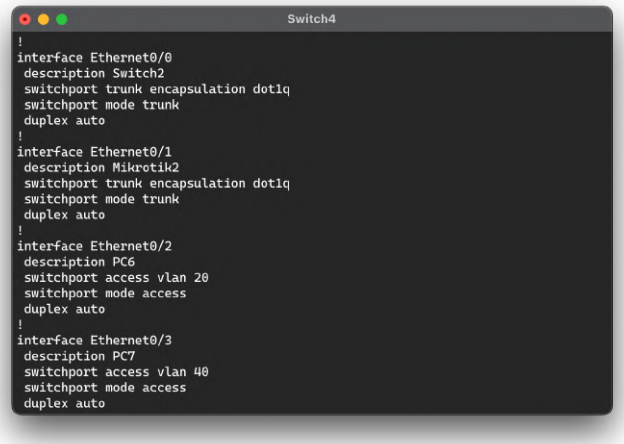

Рисунок 14 — Вывод конфигурации портов на Switch4

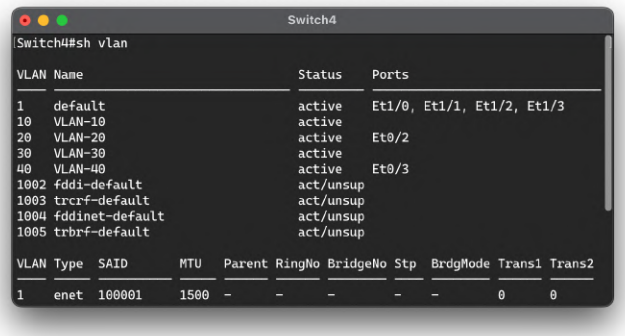

Рисунок 15 — Вывод конфигурации VLAN на Switch4

2.4 Настройка маршрутизаторов Mikrotik

Сперва был настроен маршрутизатор Mikrotik2. Вручную были

добавлены все ранее созданные VLAN, а затем был создан мост между интерфейсом VLAN-10 и соответствующими портами маршрутизатора (eth2, eth3, eth4) (рисунок 16).

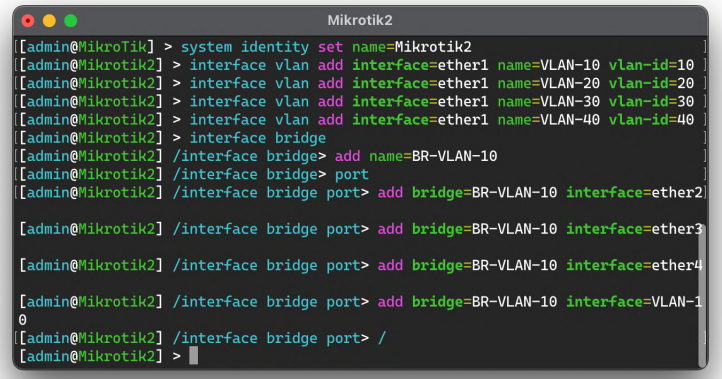

Рисунок 16 — Добавление VLAN на Mikrotik2. Настройка моста для VLAN-10

Затем был удален ненужный DHCP-клиент и была выведена конфигурация устройства (рисунок 17).

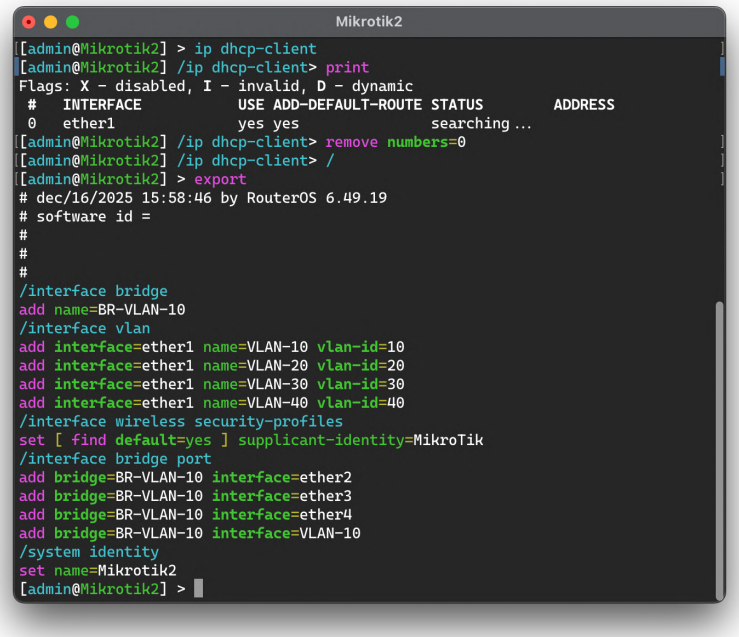

Рисунок 17 — Удаление DHCP-клиента на Mikrotik2. Вывод конфигурации

Далее был настроен маршрутизатор Mikrotik1. Он должен выполнять роль DHCP-сервера, объединяющего все VLAN и предоставляющего

доступ в интернет (рисунки 18–19).

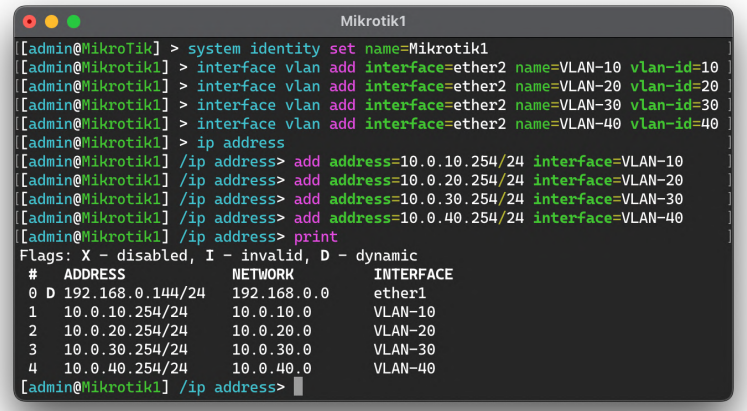

Рисунок 18 — Добавление VLAN на Mikrotik1. Настройка Gateway IP-адресов для каждого VLAN

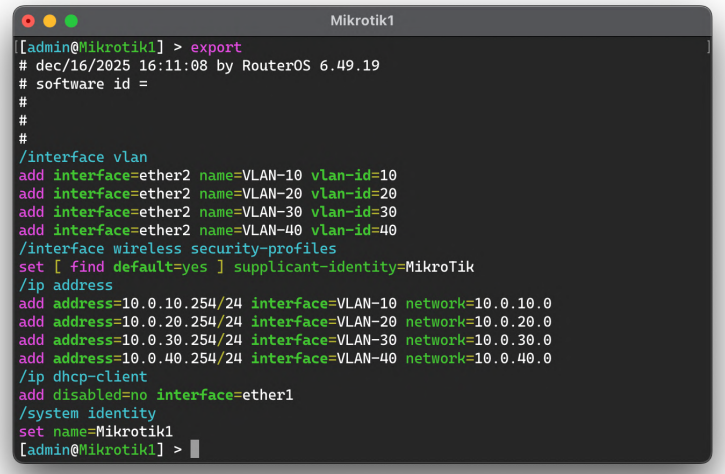

Рисунок 19 — Вывод конфигурации Mikrotik1

Теперь необходимо настроить непосредственно DHCP-сервер на Mikrotik1. Для начала нужно было настроить и вывести настройки DHCP-клиента Mikrotik1 для доступа в интернет через локальную сеть домашнего роутера (рисунок 20).

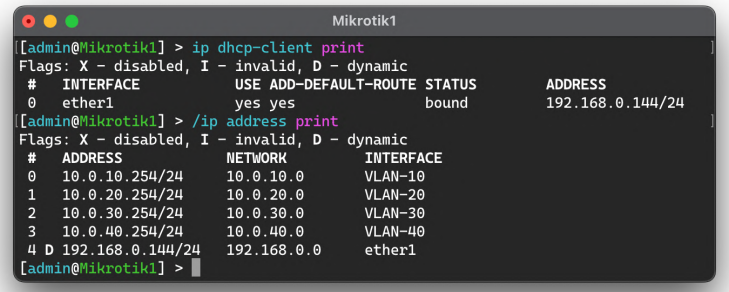

Рисунок 20 — Вывод конфигурации DHCP-клиента и IP-адресов на Mikrotik1

Далее, подключившись к маршрутизатору с помощью WinBox, необходимо определить пул IP-адресов, которые можно раздавать (рисунок 21).

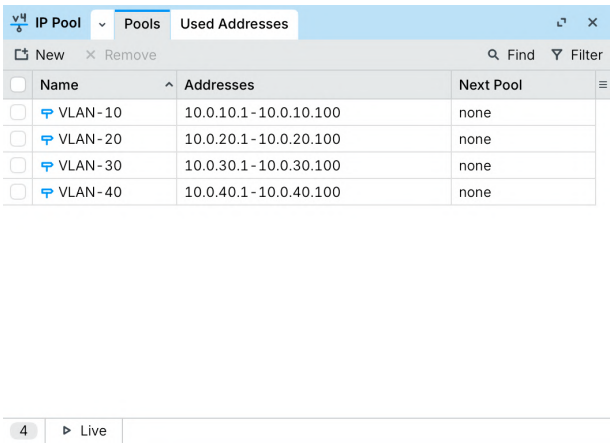

Рисунок 21 — Определение пула IP-адресов на Mikrotik1

Далее необходимо указать, в каких сетях будут находиться DHCP-сервера (для каждой VLAN), затем создать и включить сами сервера (рисунки 22–23).

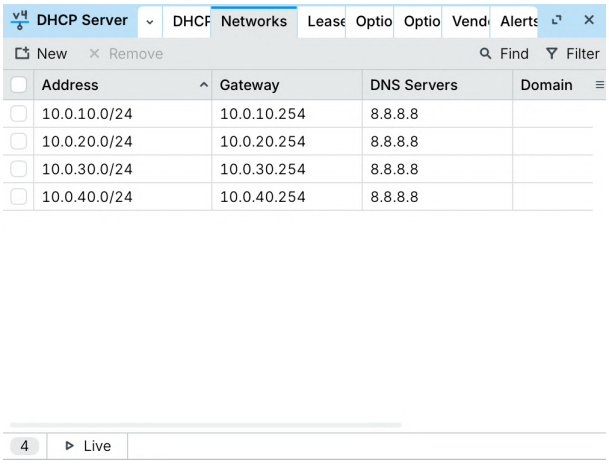

Рисунок 22 — Настройка сетей DHCP-серверов на Mikrotik1

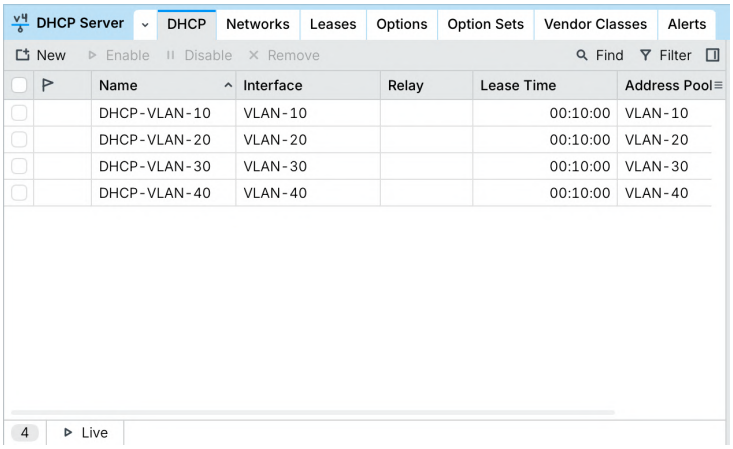

Рисунок 23 — Настройка DHCP-серверов на Mikrotik1

Теперь для проверки корректности настройки надо было вывести полную конфигурацию Mikrotik1 в консоль (рисунок 24).

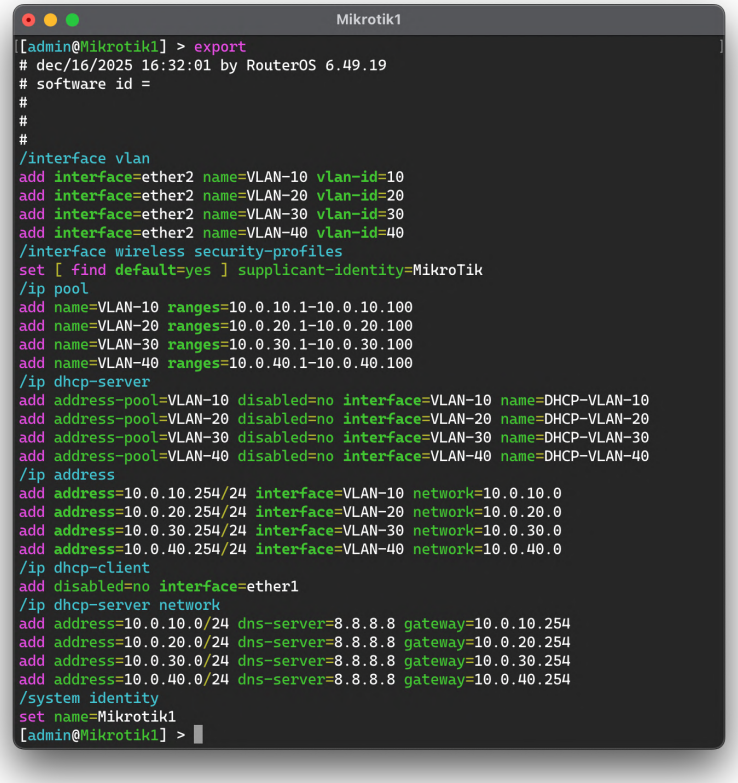

Рисунок 24 — Вывод конфигурации Mikrotik1 после настройки DHCP-серверов

Чтобы маршрутизатор Mikrotik1 знал, как обрабатывать трафик для раздачи доступа в интернет клиентам, необходимо настроить srcnat (Source NAT) NAT- правило — правило, заменяющее IP-адрес отправителя пакета с локального на публичный (общедоступный) (рисунок 25).

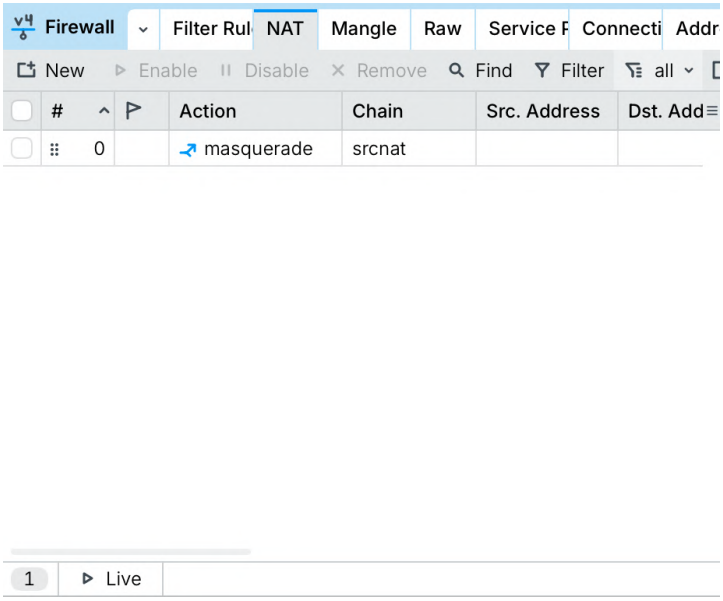

Рисунок 25 — Добавленное NAT-правило на Mikrotik1

2.5 Настройка VPCS и проверка наличия связи между компонентами

Для настройки VPCS достаточно поменять имя хоста каждой машины на соответствующее имя узла, а также запросить динамический IP-адрес у DHCP-сервера Mikrotik1 (рисунок 26).

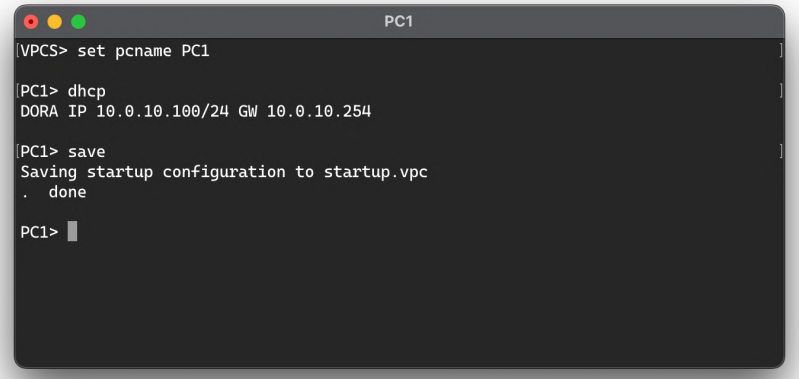

Рисунок 26 — Настройка PC1

Аналогичным образом были настроены PC2–PC7. Наконец, необходимо убедиться в наличии связи между PC4 и PC6 внутри VLAN-20 (рисунок 27).

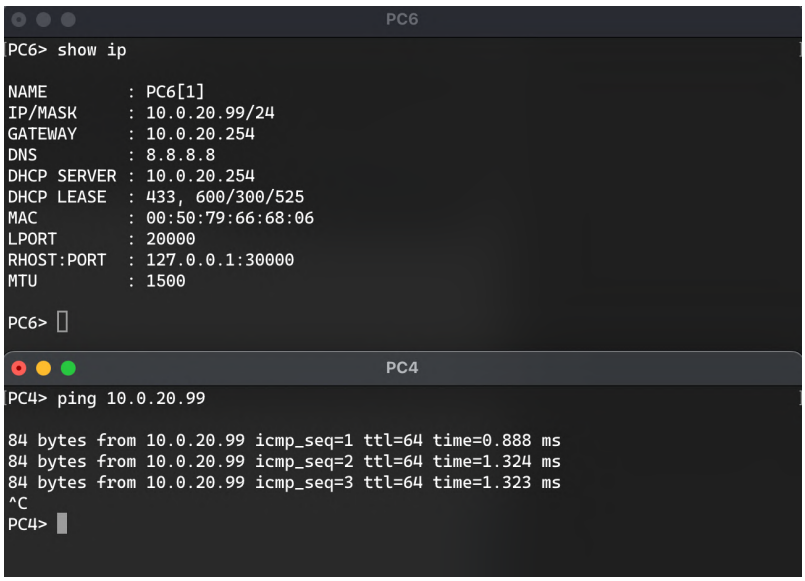

Рисунок 27 — Проверка связи внутри VLAN-20

Также нужно проверить связь между PC1 и PC3 внутри VLAN-10 (рисунок 28).

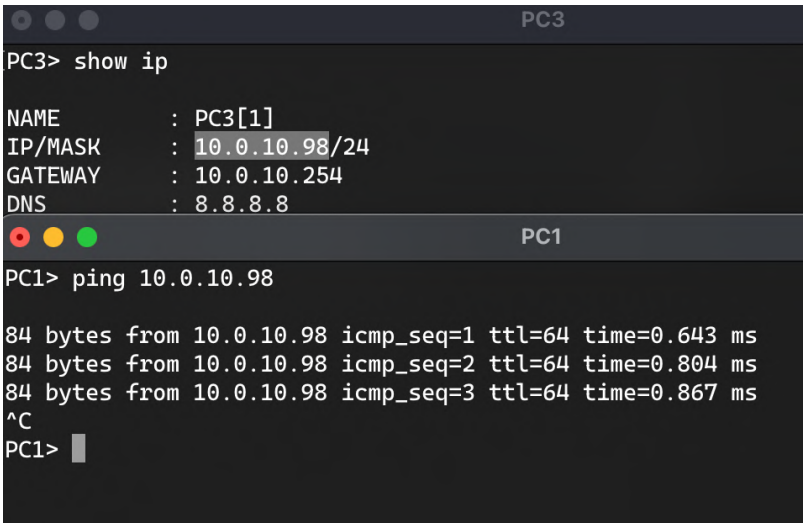

Рисунок 28 — Проверка связи внутри VLAN-10

Далее была проверена связь между PC5 в VLAN-30 и PC7 в VLAN-40 (рисунок 29).

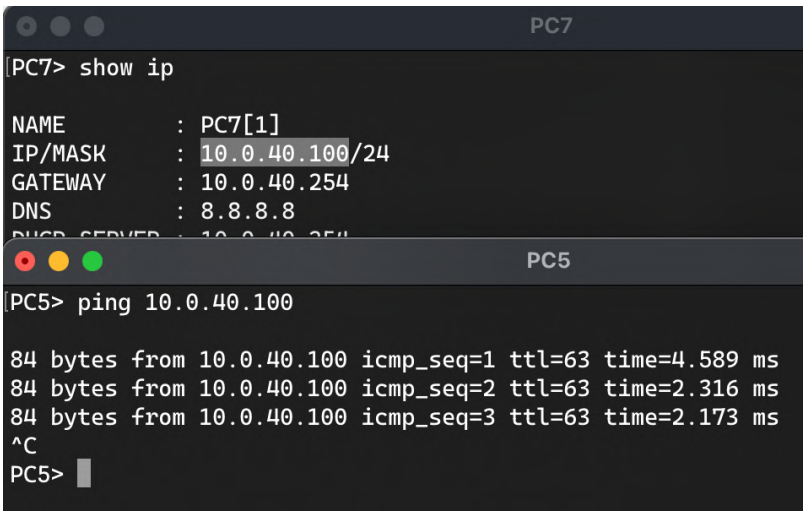

Рисунок 29 — Проверка связи между VLAN-30 и VLAN-40

И наконец, было проверено наличие связи PC2 в VLAN-10, а также PC7 в VLAN-40 с интернетом (рисунки 30–31).

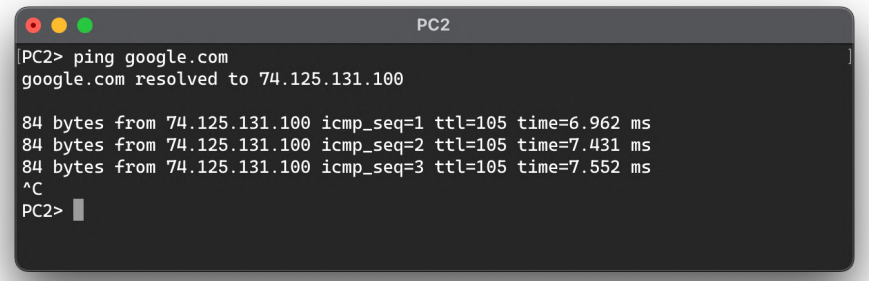

Рисунок 30 — Проверка доступа в интернет из VLAN-10

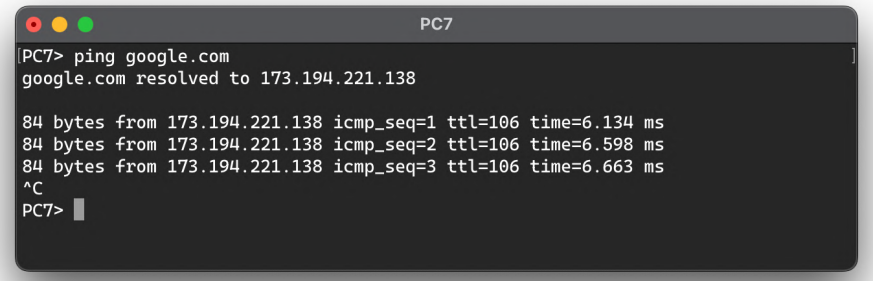

Рисунок 31 — Проверка доступа в интернет из VLAN-40

ЗАКЛЮЧЕНИЕ

В ходе выполнения курсовой работы была создана модель компьютерной сети на виртуальном стенде в соответствии с заданной топологией. Были определены характеристики используемого сетевого оборудования и реализована карта сети, отражающая структуру соединений между коммутаторами, маршрутизаторами и конечными узлами.

В процессе работы были настроены коммутаторы Cisco IOL Switch, включая конфигурацию VLAN и параметров коммутации, а также маршрутизаторы Mikrotik, обеспечивающие маршрутизацию между сегментами сети и доступ к сети Интернет. Отдельное внимание было уделено корректной настройке сетевых интерфейсов и служб, необходимых для стабильного взаимодействия всех компонентов сети.

Для проверки работоспособности модели были использованы виртуальные узлы VPCS, с помощью которых была подтверждена наличие связи внутри одного VLAN, между различными VLAN, а также доступ к сети Интернет. Результаты тестирования показали, что все элементы сети функционируют корректно, а поставленная цель курсовой работы была полностью достигнута.

Выполнение данной работы позволило закрепить практические навыки проектирования и настройки локальных сетей, а также получить опыт работы с оборудованием Cisco и Mikrotik в условиях, приближенных к реальной сетевой инфраструктуре.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Таненбаум, Э. С. Компьютерные сети / Э. С. Таненбаум, Д. Уэзеролл. — 5-е изд. — СПб.: Питер, 2016. — 960 с.

2. Odom, W. Cisco CCNA 200-301 Official Cert Guide. Volume 1 / W. Odom. — Indianapolis: Cisco Press, 2020. — 1024 p.

3. Документация MikroTik: настройка маршрутизации, NAT и DHCP / MikroTik, 2024. — URL: https://help.mikrotik.com/docs/ (дата обращения: 12.12.2025)