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

КАФЕДРА ИНФОРМАЦИОННО-СЕТЕВЫХ ТЕХНОЛОГИЙ

КУРСОВАЯ РАБОТА (ПРОЕКТ)
ЗАЩИЩЕНА С ОЦЕНКОЙ

РУКОВОДИТЕЛЬ

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

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К КУРСОВОЙ РАБОТЕ

ПОСТРОЕНИЕ ЛОКАЛЬНОЙ СЕТИ

по дисциплине: ИНФОКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. № 4329		Д.С. Шаповалова
	подпись, дата	инициалы, фамилия

Санкт-Петербург 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы данного курсового проекта обусловлена фундаментальной ролью инфокоммуникационных систем и сетей в формировании современной цифровой экономики и информационного общества. Эти системы, представляющие собой конвергентное единство телекоммуникационных сетей, вычислительных платформ и информационно-сервисных технологий, составляют критическую инфраструктуру для передачи, хранения и обработки данных. Динамичное развитие технологий, таких как 5G/6G, интернет вещей (IoT), облачные и граничные вычисления (Edge Computing), предъявляет новые требования к пропускной способности, задержкам, безопасности и масштабируемости сетей. В этих условиях проектирование, анализ и оптимизация работы сетевых инфраструктур перестают быть сугубо технической задачей, превращаясь в стратегический фактор эффективности бизнеса, государственного управления и социальных коммуникаций.

Степень научной разработанности проблемы характеризуется обширными теоретическими и практическими исследованиями в области сетевых архитектур, протоколов передачи данных и методов управления трафиком. Классические труды по модели OSI и TCP/IP, теориям коммутации и маршрутизации, созданные такими организациями, как IETF и IEEE, легли в основу современных стандартов. Однако непрерывная эволюция технологий, появление новых парадигм (таких как SDN и NFV) и рост сложности сетевых экосистем порождают постоянный поток научных изысканий, направленных на решение проблем обеспечения качества обслуживания (QoS), информационной безопасности и энергоэффективности.

Целью курсовой работы является проектирование и конфигурация сегмента корпоративной инфокоммуникационной сети, отвечающей заданным требованиям по функциональности, производительности и безопасности.

Для достижения поставленной цели необходимо решить

следующие **задачи**:

1. Проанализировать техническое задание и выделить ключевые требования к сети (логическая структура, планируемые сервисы, количество пользователей, политики безопасности).
2. Разработать логическую и физическую архитектуру сети, включая схему IP-адресации, выбор протоколов маршрутизации и планирование VLAN.
3. Смоделировать или виртуально развернуть сетевую инфраструктуру с использованием специализированного ПО (например, Cisco Packet Tracer, GNS3, Eve-NG или аппаратных решений MikroTik/Cisco).
4. Произвести детальную настройку активного сетевого оборудования (маршрутизаторов, коммутаторов) для обеспечения связности, фильтрации трафика (ACL, Firewall) и базовых сетевых служб (DHCP, NAT).
5. Провести тестирование функционирования сети: верификацию связности между сегментами, проверку корректности маршрутизации, анализ работы механизмов безопасности и трансляции адресов.
6. Оценить результаты проектирования, выявить потенциальные узкие места и сформулировать рекомендации по развитию сети.

Объект исследования – процесс проектирования и построения сегментированной корпоративной локально-вычислительной сети (ЛВС).

Предмет исследования – методы и технологии конфигурирования сетевого оборудования, протоколы взаимодействия и политики управления трафиком в инфокоммуникационной системе.

Методологическую основу работы составляют общепризнанные стандарты и руководства по построению сетей (Cisco Network Design, рекомендации IEEE), методы системного анализа, моделирования и экспериментального тестирования в лабораторной среде.

Теоретическая и практическая значимость работы заключается в консолидации теоретических знаний по курсу «Инфокоммуникационные

системы и сети» и их применении для решения практической инженерной задачи. Разработанный проект и его обоснование могут служить прототипом для развертывания реальных сетевых решений в малых и средних предприятиях.

Структура работы обусловлена последовательностью решения поставленных задач и включает введение, теоретическую главу, главу проектирования и реализации, главу тестирования и анализа, заключение, список использованных источников и приложения.

1 Индивидуальное задание

Цель работы: создать модель сети на стенде по заданной топологии.

Работа должна содержать скрины с настройкой всех компонентов (если несколько компонентов настраивались аналогично, можно представить только один скрин и написать в отчете какие компоненты настраивались аналогично), доказательства наличия связи компонентов внутри одного VLAN, между разными VLAN и интернетом.

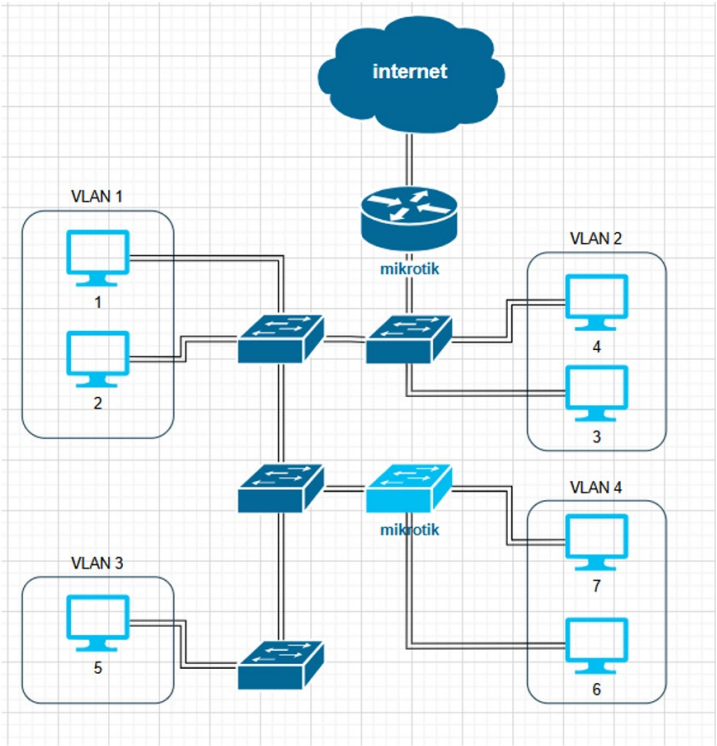

Рисунок 1 – Заданная топология сети, вариант 6

2 Выполнение задания

2.1 Настройка коммутаторов – создание VLAN.

Были выставлены в рабочую область все необходимые устройства: Router – MikroTik7.16-1 2 шт., Switch – Cisco IOU 4 шт., ПК 7 шт.

После этого началась настройка Switch 1: было установлено имя устройства и созданы VLAN.

Конфигурация представлена на рисунке 2.1:

```
IOU1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU1(config)#hostname Switch-1
Switch-1(config)#vlan 2
Switch-1(config-vlan)#name VLAN-2
Switch-1(config-vlan)#vlan 3
Switch-1(config-vlan)#name VLAN-3
Switch-1(config-vlan)#vlan 4
Switch-1(config-vlan)#name VLAN-4
Switch-1(config-vlan)#vlan 1
Switch-1(config-vlan)#name VLAN-1
%Default VLAN 1 may not have its name changed.
Switch-1(config-vlan)#exit
Switch-1(config)#exit
Switch-1#
*Dec 15 21:45:03.468: %SYS-5-CONFIG_I: Configured from console by console
Switch-1#
```

Рисунок 2.1 – Создание VLAN

Вывод информации о созданных VLAN на рисунке 2.2:

```
Switch-1#show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/2, Et0/3, Et1/0
                                                Et1/1, Et1/2, Et1/3, Et2/0
                                                Et2/1, Et2/2, Et2/3, Et3/0
                                                Et3/1, Et3/2, Et3/3
2    VLAN-2                           active
3    VLAN-3                           active
4    VLAN-4                           active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
4    enet  100004     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Рисунок 2.2 – Вывод информации о VLAN

Были настроены порты в коммутаторах. Пример настройки на Switch-2 представлен на рисунке 2.3:

```
Switch-2#
Switch-2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch-2(config)#int e0/0
Switch-2(config-if)#description Switch-1
Switch-2(config-if)#switchport trunk encapsulation
% Incomplete command.

Switch-2(config-if)#switchport trunk encapsulation dot1q
Switch-2(config-if)#switchport mode trunk
Switch-2(config-if)#exit
Switch-2(config)#int e0/2
Switch-2(config-if)#description PC1
Switch-2(config-if)#switchport mode access
Switch-2(config-if)#switchport access vlan 1
Switch-2(config-if)#exit
Switch-2(config)#int e0/3
Switch-2(config-if)#description PC2
Switch-2(config-if)#switchport mode access
Switch-2(config-if)#switchport access vlan 1
Switch-2(config-if)#exit
Switch-2(config)#
```

Рисунок 2.3 – Настройка Switch-2

Процесс был автоматизирован путём создания и настройки VTP-сервера – Switch-1, другие коммутаторы переведены в режим клиентов VTP.

Настройка сервера представлена на рисунке 3.1:

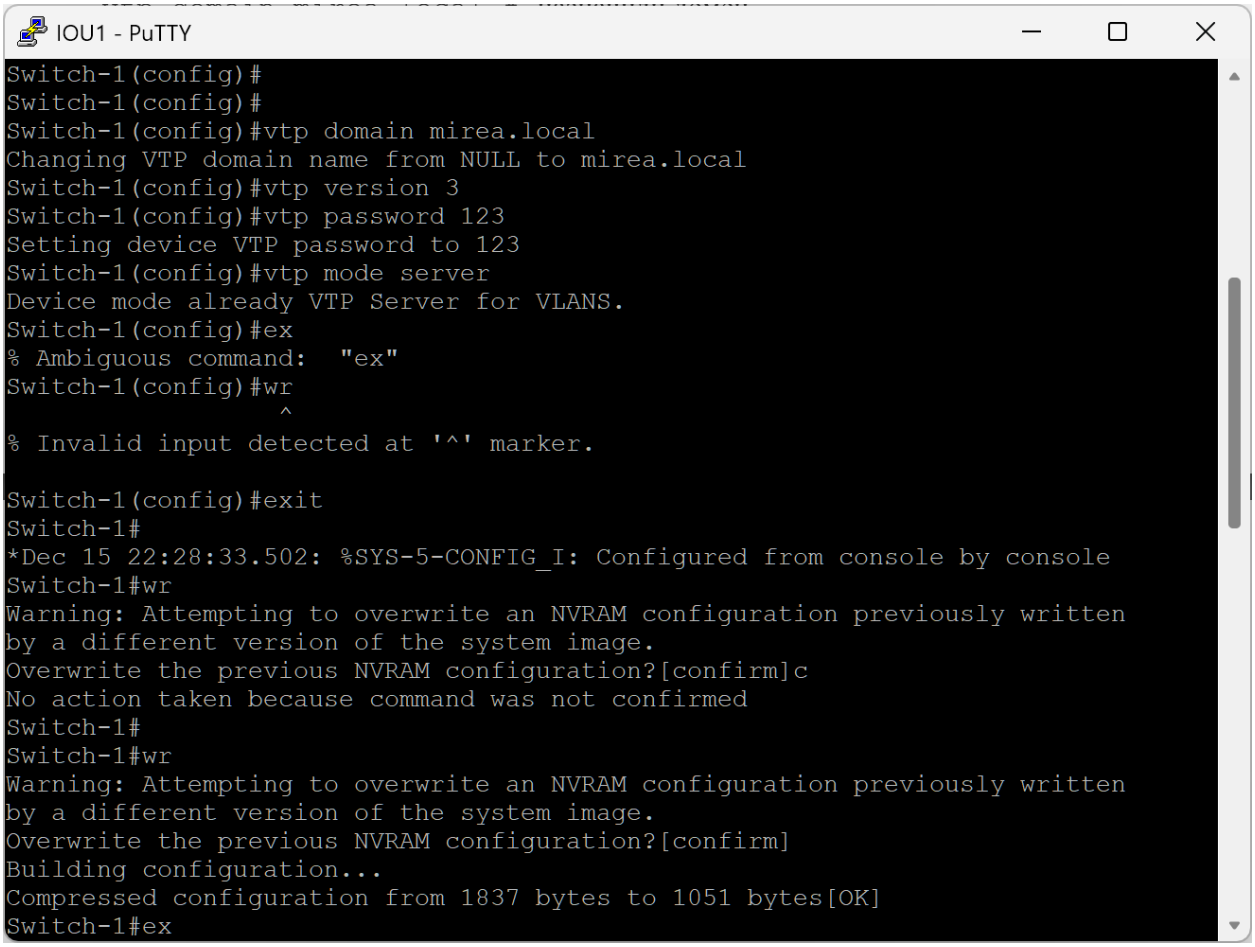

Рисунок 3.1 – Настройка VTP сервера

Было необходимо обязательно установить Switch-1, настроенный как VTP-сервер в качестве основного VTP-сервера, командой: vtp primary.

VTP статус коммутатора представлен на рисунке 3.2:

```
Switch-1(config)#exit
Switch-1#
*Dec 16 02:53:37.280: %SYS-5-CONFIG_I: Configured from console by console
Switch-1#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : mirea.local
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0100

Feature VLAN:
--------------
VTP Operating Mode                : Primary Server
Number of existing VLANs          : 9
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 4096
Configuration Revision            : 2
Primary ID                        : aabb.cc00.0100
Primary Description               : Switch-1
MD5 digest                        : 0x7B 0x3E 0xAB 0x43 0x01 0x07 0x03 0x53
                                    0x3A 0x95 0x61 0xB9 0xC3 0x2F 0x6C 0xF1


Feature MST:
--------------
VTP Operating Mode                : Transparent


Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
```

Рисунок 3.2 – Вывод информации о VTP сервере

На рисунке 3.3 показана настройка и итоговая конфигурация VTP-клиента Switch-2, оставшиеся коммутаторы настроены аналогично:

```
Switch-2(config)#vtp version 3
Switch-2(config)#vtp password 123
Setting device VTP password to 123
Switch-2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
Switch-2(config)#ex
% Ambiguous command:  "ex"
Switch-2(config)#exit
Switch-2#
*Dec 15 22:33:54.692: %SYS-5-CONFIG_I: Configured from console by console
Switch-2#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
Compressed configuration from 1528 bytes to 883 bytes[OK]
```

Рисунок 3.3 – Настройка VTP-клиента

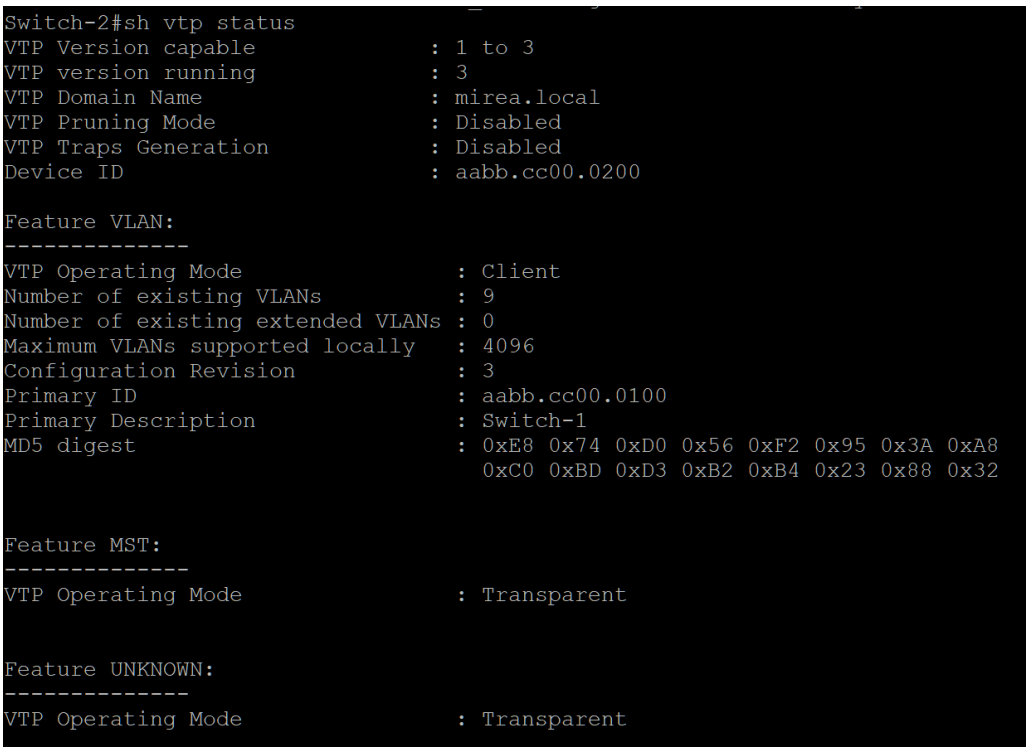

Рисунок 3.4 – Статус VTP-клиента

Настройка связи сервера и клиента по VTP-протоколу позволяет автоматически иметь информацию о имеющихся VLAN в пределах одной VTP-сети. Все манипуляции с VLAN производятся на сервере, клиенты синхронизируют конфигурацию.

Далее была проведена настройка портов на коммутаторах: для связи с ПК режим передачи устанавливается, как access (передача нетегированного трафика), для связи с другими коммутаторами – trunk (режим тегированного трафика).

Настройка Switch 1 представлена на рисунке 4.1:

```
Switch-1(config-if)#ex
Switch-1(config)#int e0/2
Switch-1(config-if)#description PC4
Switch-1(config-if)#switchport access VLAN-2
                                            ^
% Invalid input detected at '^' marker.

Switch-1(config-if)#switchport access vlan 2
Switch-1(config-if)#switchport mode access
Switch-1(config-if)#ex
Switch-1(config)#int e0/3
Switch-1(config-if)#description PC3
Switch-1(config-if)#switchport access vlan 2
Switch-1(config-if)#switchport mode access
Switch-1(config-if)#ex
Switch-1(config)#int e0/1
Switch-1(config-if)#description Switch-2
Switch-1(config-if)#switchport trunk encapsulation dot1q
Switch-1(config-if)#switchport mode trunk
Switch-1(config-if)#ex
Switch-1(config)#int e0/0
Switch-1(config-if)#description MikroTikCHR7.16-1
Switch-1(config-if)#switchport trunk encapsulation dot1q
Switch-1(config-if)#switchport mode trunk
*Dec 15 22:21:44.555: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
Switch-1(config-if)#switchport mode trunk
*Dec 15 22:21:47.568: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
```

Рисунок 4.1 – Настройка портов для Switch-1

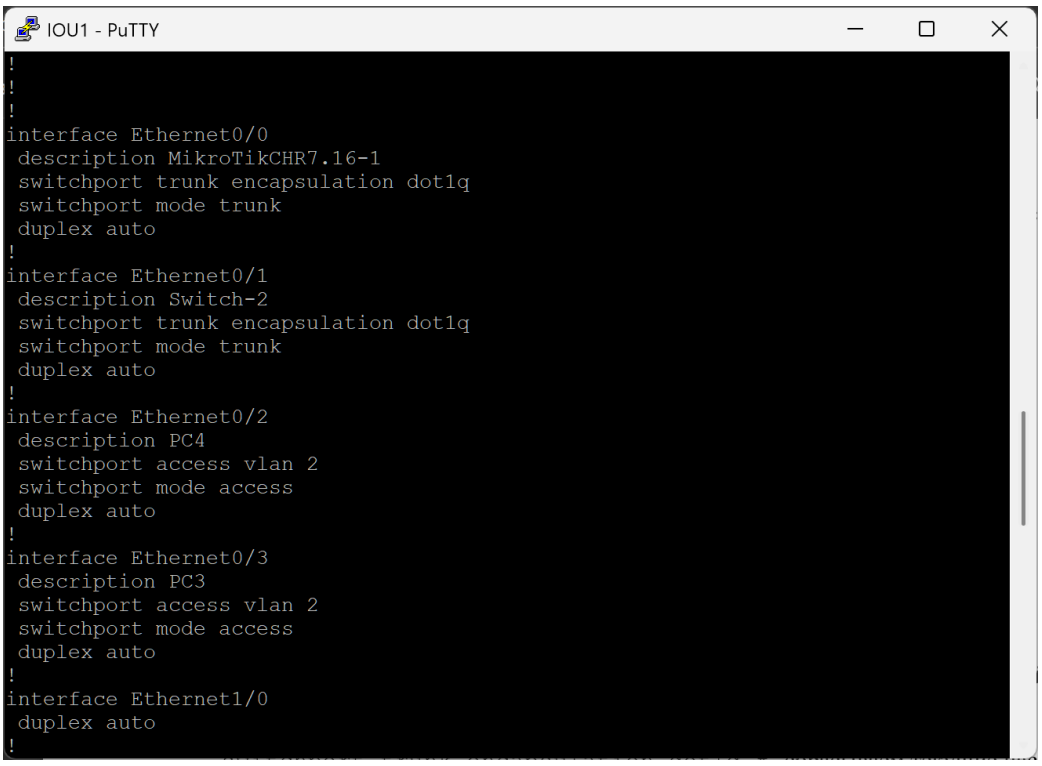

Рисунок 4.2 – Конфигурация Switch-1

Проверка корректности работы VTP-протокола и распределения VLAN была проведена посредством установки статического ip-адреса на ПК и

выполнения команды ping между компьютерами в одной VLAN, в разных VLAN.

Результат представлен на рисунке 5:

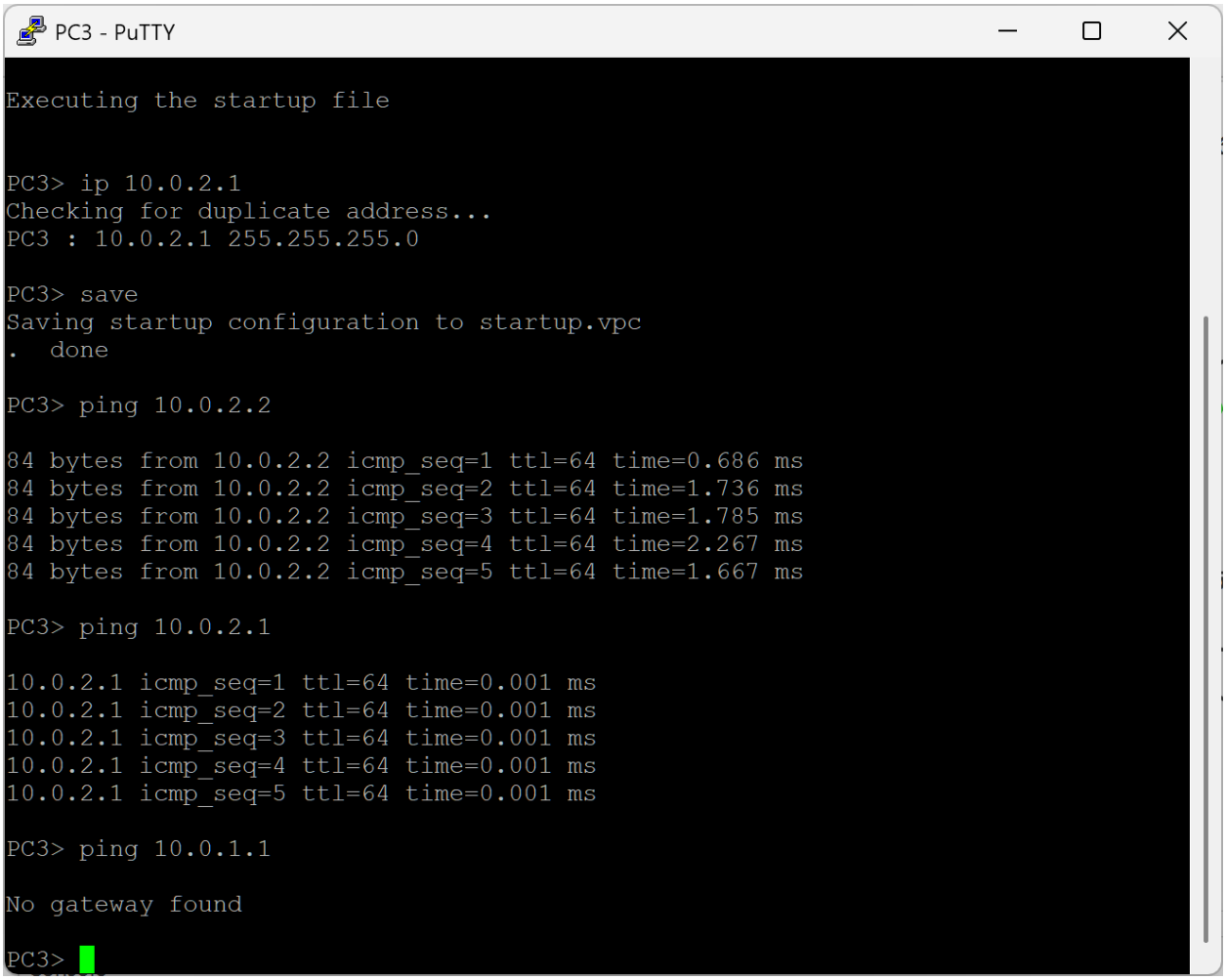

Рисунок 5 – Проверка работы VLAN, ping

2.2 Настройка маршрутизатора и моста

Согласно схеме для связи PC7 и PC6 (VLAN 4) с остальными участниками сети необходимо использовать устройство типа MikroTik. Его настройка отличается от настройки коммутаторов Cisco.

Настройка была проведена отдельно и представлена на рисунке 6.1:

```
[admin@MikroTik] > system identity set name=MikroTik-2
[admin@MikroTik-2] > interface vlan add interface=ether1 name=default vlan-id=1
[admin@MikroTik-2] > interface vlan add interface=ether1 name=VLAN-2 vlan-id=2
[admin@MikroTik-2] > interface vlan add interface=ether1 name=VLAN-3 vlan-id=3
[admin@MikroTik-2] > interface vlan add interface=ether1 name=VLAN-4 vlan-id=4
[admin@MikroTik-2] > interface bridge
[admin@MikroTik-2] /interface/bridge> add name=BR-VLAN-4
[admin@MikroTik-2] /interface/bridge> port
[admin@MikroTik-2] /interface/bridge/port> add bridge= BR-VLAN-4 interface=ether
2
[admin@MikroTik-2] /interface/bridge/port> add bridge= BR-VLAN-4 interface=VLAN-
4
[admin@MikroTik-2] /interface/bridge/port> ..
[admin@MikroTik-2] /interface/bridge> /
[admin@MikroTik-2] > export
```

Рисунок 6.1 – Настройка MikroTik-2 с мостом

На коммутаторе настраивается интерфейс моста для объединения VLAN 4, созданной на интерфейсе порта ether1, с портом ether2 и ether3 (дописана команда /interface bridge port add bridge=BR-VLAN-4 interface=ether3).

Полученная конфигурации MikroTik 2 представлена на рисунке 6.2:

```
-2] > export ik-2] > export
# 2025-12-16 00:16:21 by RouterOS 7.16 port add bridge=BR-VLAN-4 interface=ether3
# software id =
#
/interface bridge
add name=BR-VLAN-4
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no
set [ find default-name=ether2 ] disable-running-check=no
set [ find default-name=ether3 ] disable-running-check=no
set [ find default-name=ether4 ] disable-running-check=no
set [ find default-name=ether5 ] disable-running-check=no
set [ find default-name=ether6 ] disable-running-check=no
set [ find default-name=ether7 ] disable-running-check=no
set [ find default-name=ether8 ] disable-running-check=no
/interface vlan
add interface=ether1 name=VLAN-2 vlan-id=2
add interface=ether1 name=VLAN-3 vlan-id=3
add interface=ether1 name=VLAN-4 vlan-id=4
add interface=ether1 name=default vlan-id=1
/port
set 0 name=serial0
/interface bridge port
add bridge=BR-VLAN-4 interface=ether2
add bridge=BR-VLAN-4 interface=VLAN-4
add bridge=BR-VLAN-4 interface=ether3
/ip dhcp-client
add interface=ether1
/system identity
set name=MikroTik-2
/system note
set show-at-login=no
[admin@MikroTik-2] >
```

Рисунок 6.2 – Конфигурация MikroTik2

Проверка была сделана путём выполнения команды ping с ПК в одной сети VLAN-4 и в разных, представлена на рисунке 6.3:

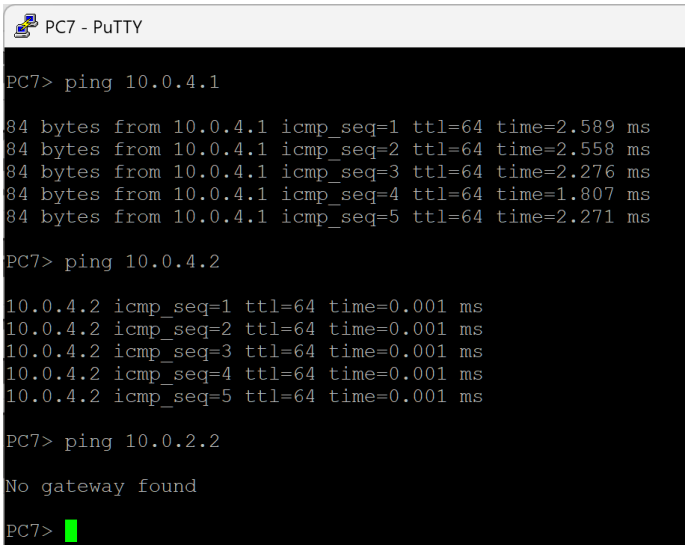

Рисунок 6.3 – Проверка работы VLAN от MikroTik

Далее была произведена настройка маршрутизатора MikroTik 1 – были созданы интерфейсы для VLAN, установлены ip адреса для каждой из сетей. Настройка представлена на рисунке 7.1 и 7.2:

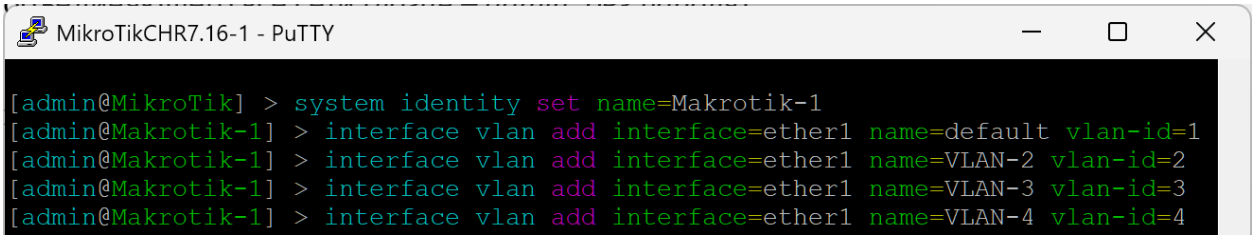

Рисунок 7.1 – Настройка VLAN интерфейсов маршрутизатора

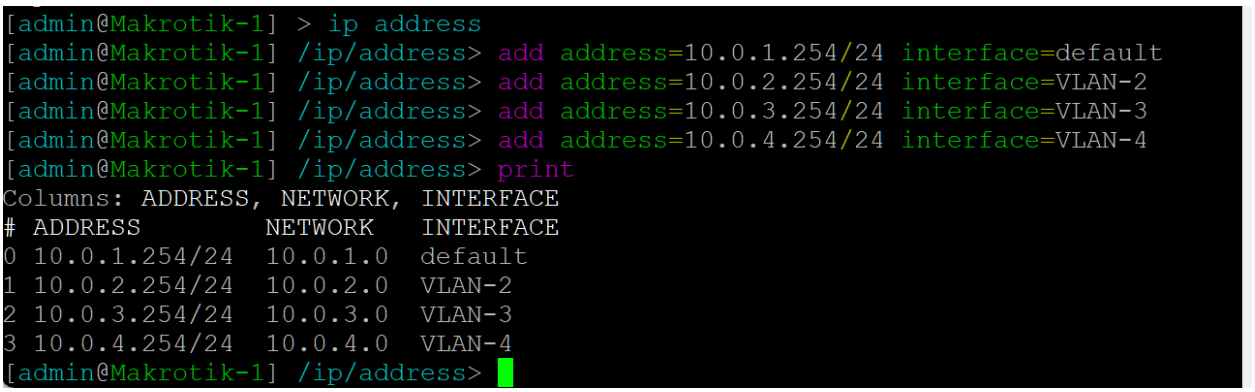

Рисунок 7.2 – Настройка ip-адресов маршрутизатора

Полученная конфигурация на рисунке 7.3:

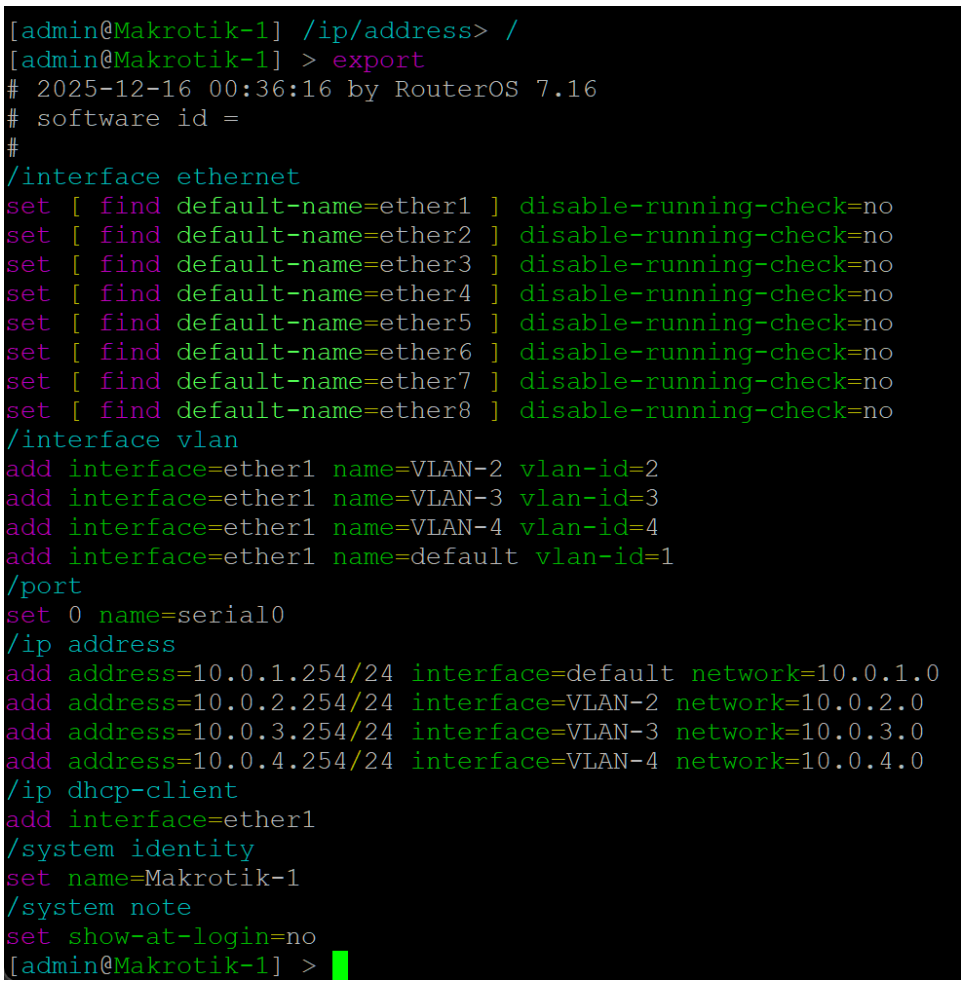

Рисунок 7.3 – Конфигурация MikroTik-1

2.3 Настройка DHCP сервера и выхода в интернет

Была проведена настройка DHCP клиента на маршрутизаторе MikroTik-1 на интерфейс ether2, а затем клиент получил адрес 192.168.122.48/24 от DHCP-сервера.

Вывод ip-адресов в консоль демонстрирует, что статические VLAN-интерфейсы имеют фиксированные адреса вида 10.0.X.254/24, гдк X – номер сети VLAN, а динамический адрес на ether2 помечен флагом D – Dynamic.

Настройка DHCP-клиента представлена на рисунке 8:

```
# INTERFACE  USE-PEER-DNS  ADD-DEFAULT-ROUTE  STATUS
0 ether1     yes           yes                searching...
[admin@Makrotik-1] /ip/dhcp-client> print
Columns: INTERFACE, USE-PEER-DNS, ADD-DEFAULT-ROUTE, STATUS
# INTERFACE  USE-PEER-DNS  ADD-DEFAULT-ROUTE  STATUS
0 ether1     yes           yes                searching...
[admin@Makrotik-1] /ip/dhcp-client> /ip dhcp-client remove numbers=0
[admin@Makrotik-1] /ip/dhcp-client> add interface=ether2
[admin@Makrotik-1] /ip/dhcp-client> print
Columns: INTERFACE, USE-PEER-DNS, ADD-DEFAULT-ROUTE, STATUS, ADDRESS
# INTERFACE  USE-PEER-DNS  ADD-DEFAULT-ROUTE  STATUS  ADDRESS
0 ether2     yes           yes                bound   192.168.122.48/24
[admin@Makrotik-1] /ip/dhcp-client> ip address print
bad command name ip (line 1 column 1)
[admin@Makrotik-1] /ip/dhcp-client> /
[admin@Makrotik-1] > ip address print
Flags: D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#   ADDRESS            NETWORK        INTERFACE
0   10.0.1.254/24      10.0.1.0       default
1   10.0.2.254/24      10.0.2.0       VLAN-2
2   10.0.3.254/24      10.0.3.0       VLAN-3
3   10.0.4.254/24      10.0.4.0       VLAN-4
4 D 192.168.122.48/24  192.168.122.0  ether2
[admin@Makrotik-1] >
```

Рисунок 8 – Настройка DHCP-клиента

Дальнейшая настройка маршрутизатора производилась с помощью программы WinBox.

Для каждой сети был создан пул ip адресов, при этом установлены исключения. Процесс создания пула и список пулов для каждой из VLAN представлены на рисунках 9.1-9.2:

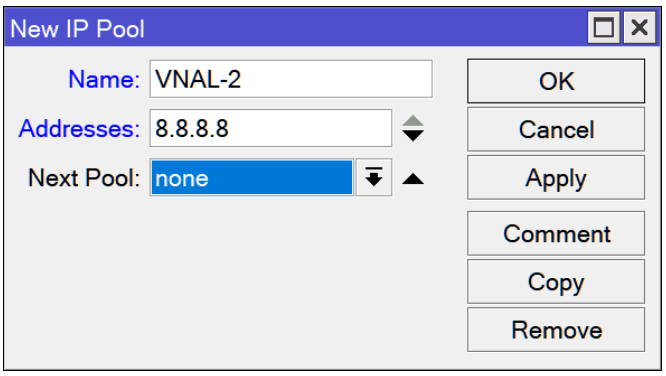

Рисунок 9.1 – Создание пула

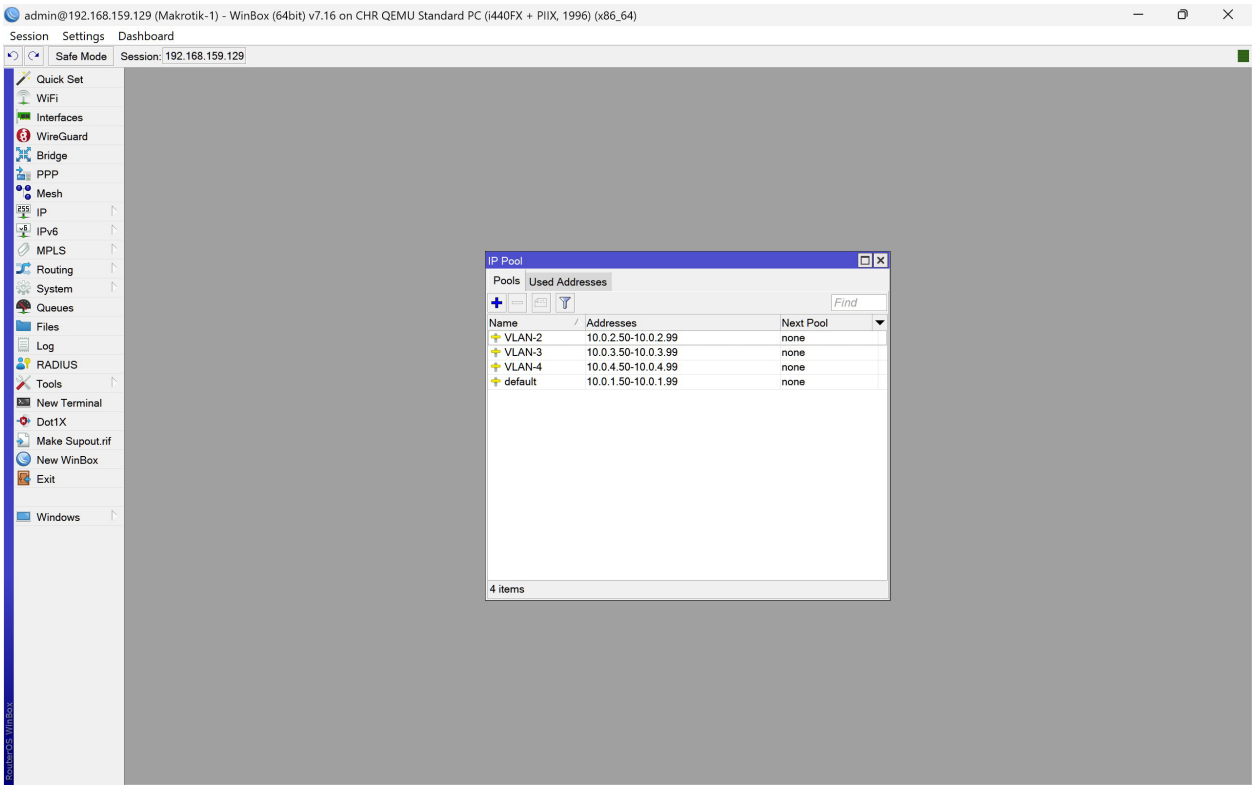

Рисунок 9.2 – Созданные ip пулы

Далее были добавлены и настроены сети, в которых будут находится DHCP- сервера.

Процесс создания сети для VLAN-1 представлен на рисунке 10.1:

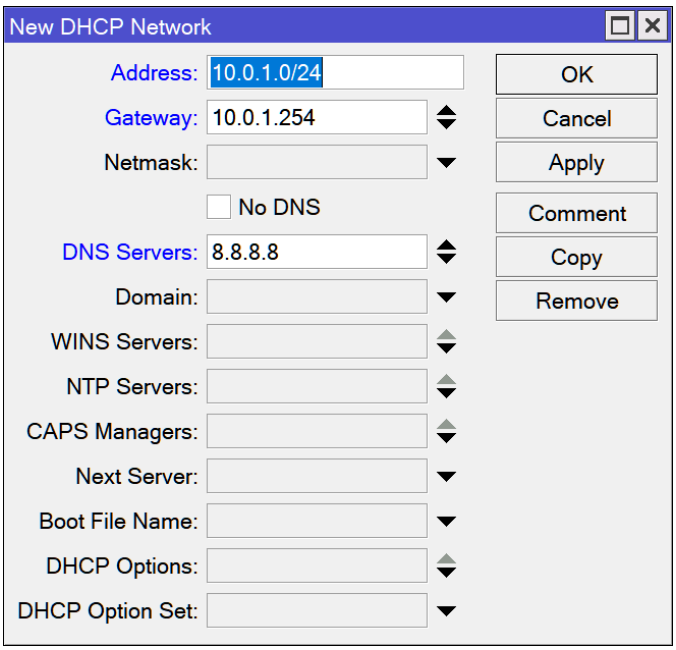

Рисунок 10.1 – Создание сети

Для каждого интерфейса VLAN были созданы и настроены DHCP сервера, процесс создания для VLAN 2 представлен на рисунке 10.2:

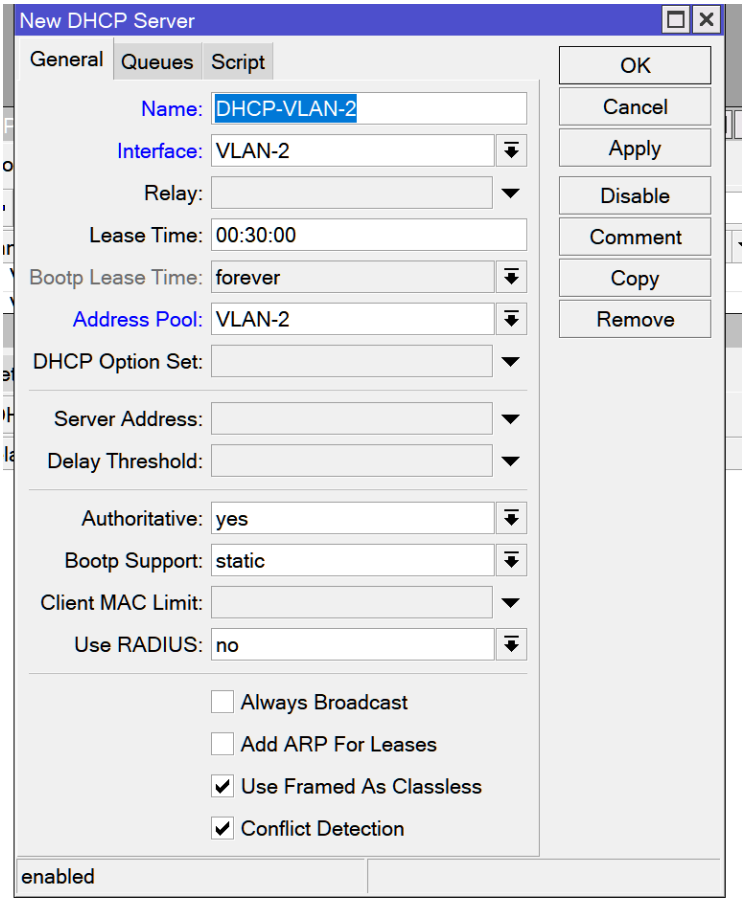

Рисунок 10.2 – Создание и настройка dhcp сервера

Созданные сети и DHCP-сервера для всех VLAN представлены на рисунках 10.3 и 10.4:

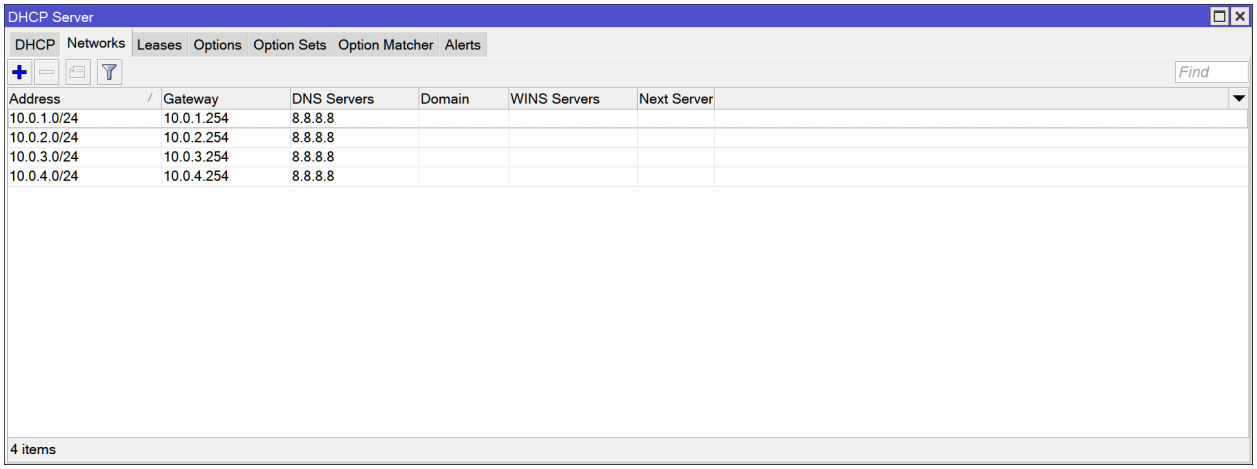

Рисунок 10.3 – Созданные сети

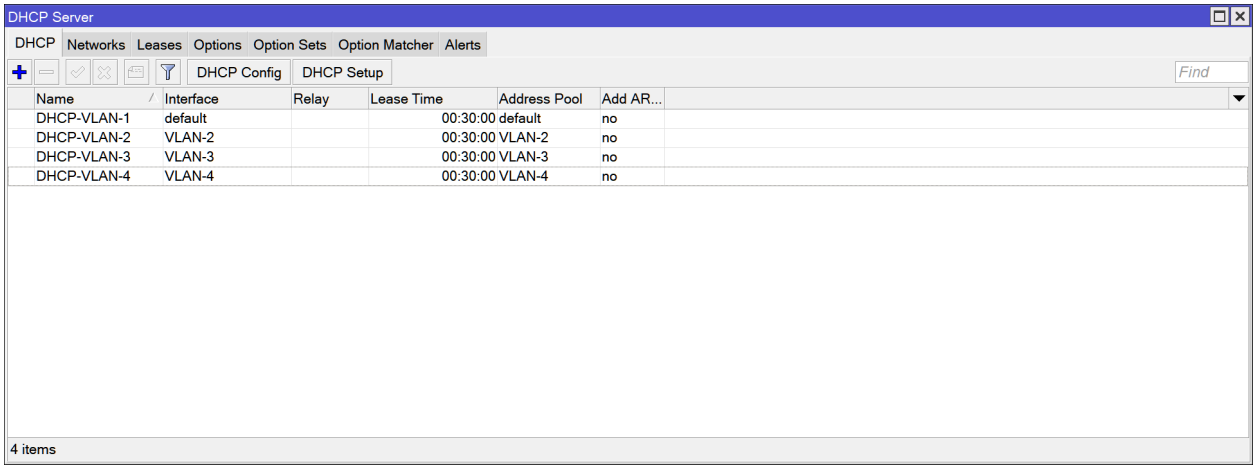

Рисунок 10.4 – Созданные dhcp сервера

Итоговая конфигурация роутера MikroTik-1 доступна к выводу при помощи команды «export» и представлена на рисунке 11. Теперь выводятся списки пулов, сетей и DHCP-серверов.

```
/interface ethernet
set [ find default-name=ether1 ] disable-running-check=no
set [ find default-name=ether2 ] disable-running-check=no
set [ find default-name=ether3 ] disable-running-check=no
set [ find default-name=ether4 ] disable-running-check=no
set [ find default-name=ether5 ] disable-running-check=no
set [ find default-name=ether6 ] disable-running-check=no
set [ find default-name=ether7 ] disable-running-check=no
set [ find default-name=ether8 ] disable-running-check=no
/interface vlan
add interface=ether1 name=VLAN-2 vlan-id=2
add interface=ether1 name=VLAN-3 vlan-id=3
add interface=ether1 name=VLAN-4 vlan-id=4
add interface=ether1 name=VLAN-10 vlan-id=10
add interface=ether1 name=default vlan-id=1
/ip pool
add name=default ranges=10.0.1.50-10.0.1.99
add name=VLAN-2 ranges=10.0.2.50-10.0.2.99
add name=VLAN-3 ranges=10.0.3.50-10.0.3.99
add name=VLAN-4 ranges=10.0.4.50-10.0.4.99
add name=VLAN-10 ranges=10.0.10.50-10.0.10.99
/ip dhcp-server
add address-pool=VLAN-2 interface=VLAN-2 name=DHCP-VLAN-2
add address-pool=default interface=default name=DHCP-VLAN-1
add address-pool=VLAN-3 interface=VLAN-3 name=DHCP-VLAN-3
add address-pool=VLAN-4 interface=VLAN-4 name=DHCP-VLAN-4
add address-pool=VLAN-10 interface=VLAN-10 name=DHCP-VLAN-10
/port
set 0 name=serial0
/ip address
add address=10.0.1.254/24 interface=default network=10.0.1.0
add address=10.0.2.254/24 interface=VLAN-2 network=10.0.2.0
add address=10.0.3.254/24 interface=VLAN-3 network=10.0.3.0
add address=10.0.4.254/24 interface=VLAN-4 network=10.0.4.0
add address=10.0.10.254/24 interface=VLAN-10 network=10.0.10.0
/ip dhcp-client
add interface=ether2
/ip dhcp-server network
add address=10.0.1.0/24 dns-server=8.8.8.8 gateway=10.0.1.254 netmask=24
add address=10.0.2.0/24 dns-server=8.8.8.8 gateway=10.0.2.254 netmask=24
add address=10.0.3.0/24 dns-server=8.8.8.8 gateway=10.0.3.254 netmask=24
add address=10.0.4.0/24 dns-server=8.8.8.8 gateway=10.0.4.254 netmask=24
add address=10.0.10.0/24 dns-server=8.8.8.8 gateway=10.0.10.254
/ip firewall filter
add action=accept chain=forward out-interface=ether2
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether2
/system identity
set name=Makrotik-1
/system note
set show-at-login=no
```

Рисунок 11 – Вывод конфигурации с MikroTik-1

Заключительной стадией конфигурации сервера на базе MikroTik, функционирующего в качестве шлюза, явилась организация трансляции сетевых адресов (NAT). Данный механизм является стандартным решением для обеспечения выхода множества узлов частной сети в глобальную

инфраструктуру Интернет посредством единого публичного IP-адреса пограничного маршрутизатора.

Принцип функционирования основан на замене приватных IP-адресов отправителей во исходящих пакетах на публичный адрес шлюза. Обратная подмена адреса назначения производится при получении ответных пакетов из внешней сети, что обеспечивает корректную маршрутизацию трафика до конкретного узла внутри локального сегмента.

Реализация в среде WinBox включала определение следующего правила преобразования:

1. В поле chain было установлено значение srcnat. Это указывает на принадлежность правила к цепочке Source NAT, предназначенной для обработки исходящего трафика, источником которого является локальная сеть. Правила данной цепочки модифицируют поле исходного адреса в IP-заголовке пакета.
2. Параметр action был определён как masquerade. Данный режим представляет собой специализированный случай динамического SNAT, при котором в качестве адреса для подмены автоматически и без явного указания используется текущий IP-адрес, назначенный внешнему интерфейсу маршрутизатора. Это обеспечивает адаптивность конфигурации при изменении внешнего адреса.
3. Критерием применения правила был задан внешний интерфейс ether2. Указание данного интерфейса является необходимым условием для селективной обработки только того трафика, который направлен во внешнюю сеть, обеспечивая корректную работу механизма трансляции адресов.

   Настройка NAT правила представлена на рисунках 12.1 и 12.2:

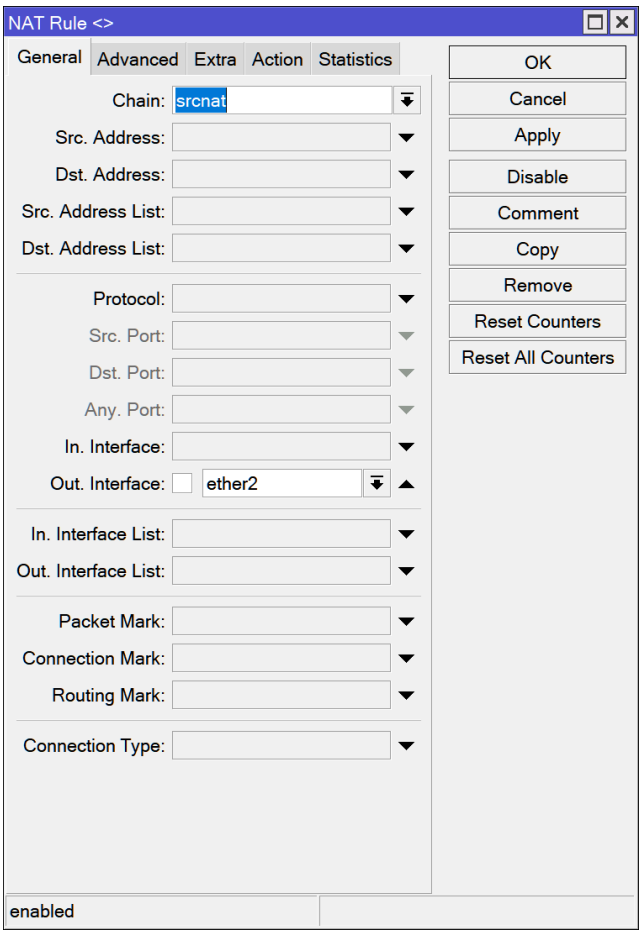

Рисунок 24 – Создание выхода в интернет

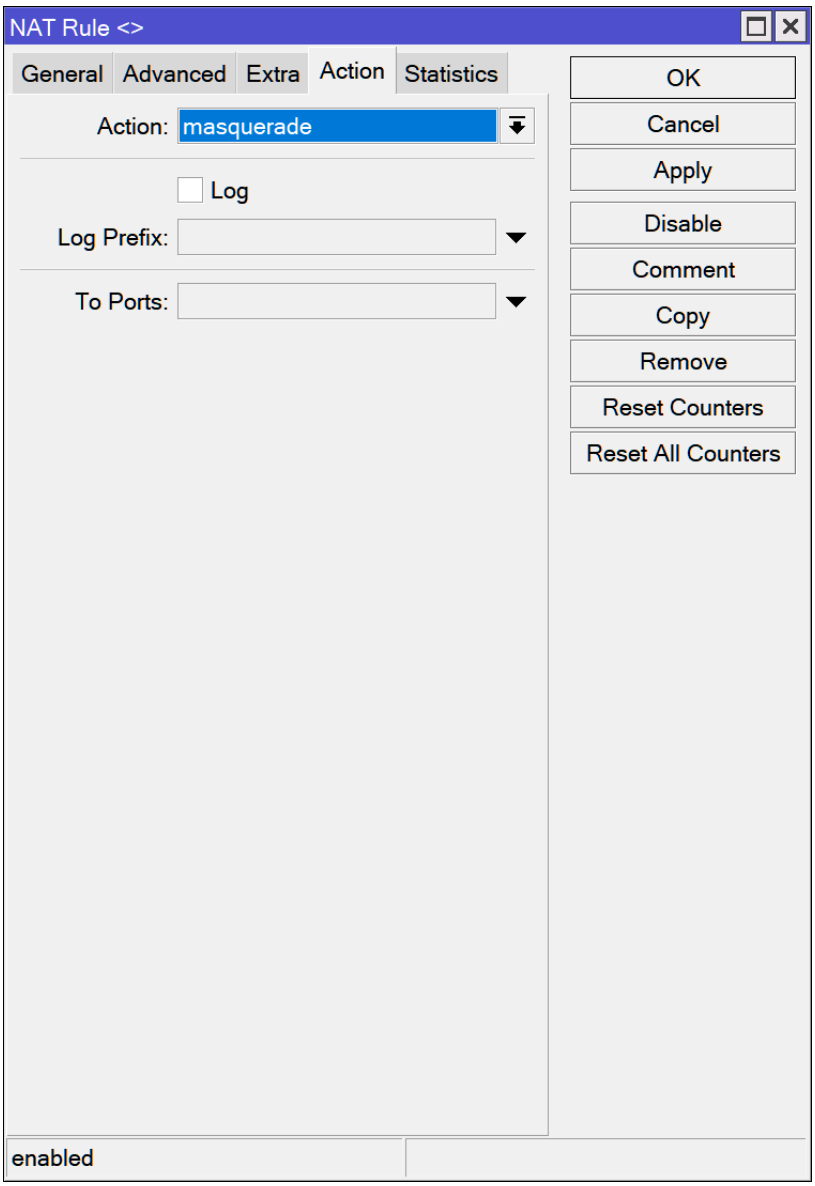

Рисунок 12.2 – Создание выхода в интернет

Отображение в списке Firewall представлено на рисунке 12.3:

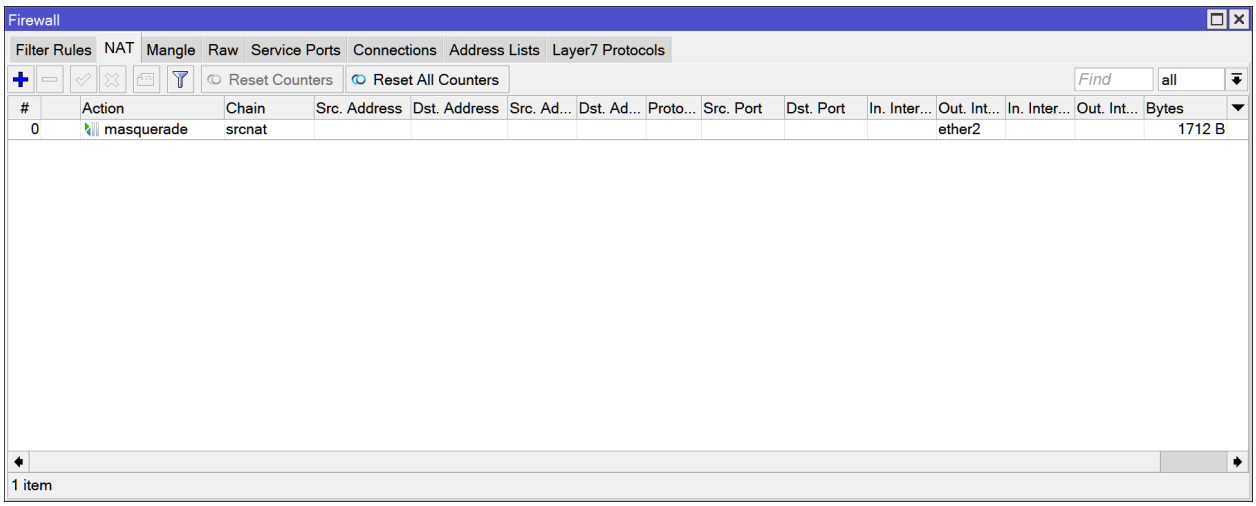

Рисунок 12.3 – Настройка NAT в Firewall

После этого всем ПК был динамически назначен ip адрес в соответствии с установленными в пуле ограничениям.

2.4 Проверка итоговой сети

С разных ПК была проведена проверка трафика при помощи команды ping. Была проверена связь между компьютерами в одной локальной сети, компьютерами из разных сетей, а также связь с интернетом (рисунки 13.1 – 13.2).

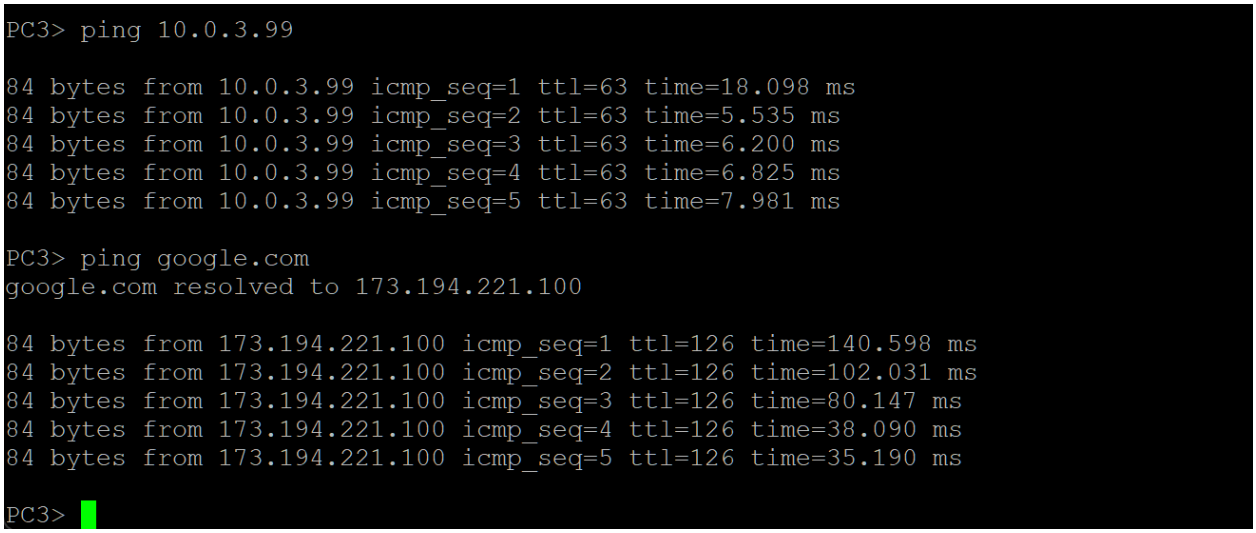

Рисунок 13.1 – ping с ПК

```
84 bytes from 173.194.221.100 icmp_seq=5 ttl=126 time=35.190 ms

PC3> sh ip

NAME        : PC3[1]
IP/MASK     : 10.0.2.98/24
GATEWAY     : 10.0.2.254
DNS         : 8.8.8.8
DHCP SERVER : 10.0.2.254
DHCP LEASE  : 1178, 1800/900/1575
MAC         : 00:50:79:66:68:02
LPORT       : 20036
RHOST:PORT  : 127.0.0.1:20037
MTU         : 1500

PC3> dhcp
DORA IP 10.0.2.98/24 GW 10.0.2.254

PC3> sh ip

NAME        : PC3[1]
IP/MASK     : 10.0.2.98/24
GATEWAY     : 10.0.2.254
DNS         : 8.8.8.8
DHCP SERVER : 10.0.2.254
DHCP LEASE  : 1797, 1800/900/1575
MAC         : 00:50:79:66:68:02
LPORT       : 20036
RHOST:PORT  : 127.0.0.1:20037
MTU         : 1500

PC3> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=126 time=126.951 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=126 time=128.412 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=126 time=82.648 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=126 time=35.978 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=126 time=37.642 ms

PC3>
```

Рисунок 13.2 – Проверка доступности

Полученная сеть представлена на рисунке 14.

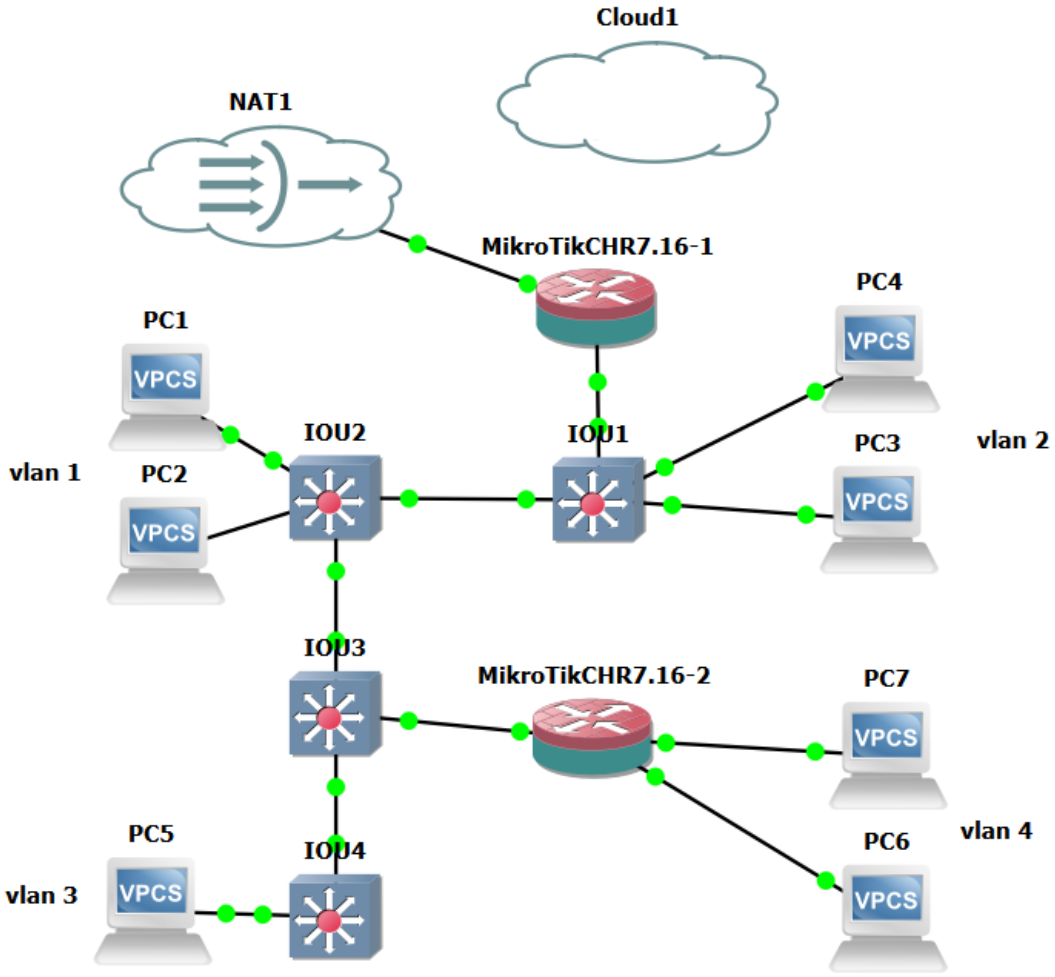

Рисунок 14 – Полученная сеть

ЗАКЛЮЧЕНИЕ

В ходе выполнения данной курсовой работы была успешно спроектирована, развернута и протестирована сегментированная локальная сеть корпоративного типа, полностью соответствующая заданной топологии и индивидуальному заданию. Основной целью работы являлось создание функциональной модели сети, объединяющей разнородное сетевое оборудование, что было достигнуто.

В процессе работы последовательно решены следующие ключевые задачи:

1. Построена логическая структура сети на основе пяти виртуальных локальных сетей (VLAN), что позволило обеспечить логическую изоляцию групп устройств по функциональному признаку и повысить безопасность.
2. Настроено активное сетевое оборудование: коммутаторы Cisco и маршрутизаторы MikroTik. Централизованное управление конфигурацией VLAN было реализовано с помощью протокола VTP, где один коммутатор выступал в роли сервера, а остальные – клиентов.
3. Осуществлена детальная настройка интерфейсов: порты, подключенные к конечным устройствам, настроены в режиме доступа (Access), а магистральные соединения (Trunk) – для передачи тегированного трафика между коммутаторами и маршрутизатором.
4. Реализована маршрутизация между VLAN по схеме «Router-on-a-Stick» на маршрутизаторе MikroTik-1, где для каждого VLAN был создан отдельный логический интерфейс с назначением IP-адреса, выступающего шлюзом для своей подсети.
5. Настроена инфраструктура динамического распределения адресов (DHCP). На маршрутизаторе созданы пулы адресов для каждого VLAN, что позволило автоматически назначать конечным устройствам IP-адреса, параметры шлюза и DNS-сервера.

6. Обеспечен выход всех сегментов сети в глобальный Интернет через единый внешний интерфейс маршрутизатора MikroTik-1 с применением технологии трансляции сетевых адресов (NAT) в режиме masquerade.

Все этапы настройки были подтверждены скриншотами конфигурации, а итоговая работоспособность сети проверена комплексно с помощью утилиты ping. Тестирование доказало:

- Наличие связности между устройствами внутри одного VLAN.
- Корректную маршрутизацию и связность между устройствами из разных VLAN.
- Успешный доступ всех сегментов сети к ресурсам глобальной сети Интернет.

Таким образом, **поставленная цель курсовой работы достигнута**. Разработанная и реализованная сетевая модель наглядно демонстрирует принципы построения современных инфокоммуникационных систем, сочетающих логическую сегментацию, динамическую адресацию, межсетевое взаимодействие и доступ к внешним ресурсам. Полученный практический опыт конфигурации оборудования различных вендоров (Cisco, MikroTik) и интеграции их в единую систему имеет высокую практическую значимость и составляет основу профессиональных компетенций в области сетевых технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Мещеряков, А. И. Проблема выбора среды моделирования для изучения сетевых технологий / А. И. Мещеряков // Молодой исследователь Дона. – 2021. – № 6(33). – с. 70-76.

2. Zyxel Support Campus EMEA: Zyxel Firewall [NAT] - Что такое NAT (трансляция сетевых адресов), URL: https://http://support.zyxel.eu/hc/ru/articles/19202116741010-Zyxel-Firewall-NAT-Что-такое-NAT-трансляция-сетевых-адресов (дата обращения: 11.12.2025).

3. Академия Selectel: DHCP-протокол: что это такое и как он работает, URL: https://selectel.ru/blog/dhcp-protocol/ (дата обращения: 11.12.2025).

4. Yandex Cloud: DNS-сервер: как работает и какие типы существуют, URL: https://yandex.cloud/ru/docs/glossary/dns?utm_referrer=https%3A%2F%2Fwww.google.com%2F&utm_referrer=about%3Ablank (дата обращения: 11.12.2025).

5. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер. – СПб: Питер, 2012. – 944 с.