

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

должность, уч. степень, звание

подпись, дата

В. М. Смирнов

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

подпись, дата

Г. С. Томчук

инициалы, фамилия

Санкт-Петербург 2025

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ И СПЕЦИАЛЬНЫХ ТЕРМИНОВ	3
ВВЕДЕНИЕ	4
1 Техническое задание	5
2 Ход выполнения работы	6
2.1 Определение характеристик оборудования.....	6
2.2 Реализация карты сети на стенде.....	6
2.3 Настройка коммутаторов Cisco IOL Switch.....	6
2.4 Настройка маршрутизаторов Mikrotik	11
2.5 Настройка VPCS и проверка наличия связи между компонентами	16
ЗАКЛЮЧЕНИЕ.....	19
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	20

СПИСОК СОКРАЩЕНИЙ И СПЕЦИАЛЬНЫХ ТЕРМИНОВ

- 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.

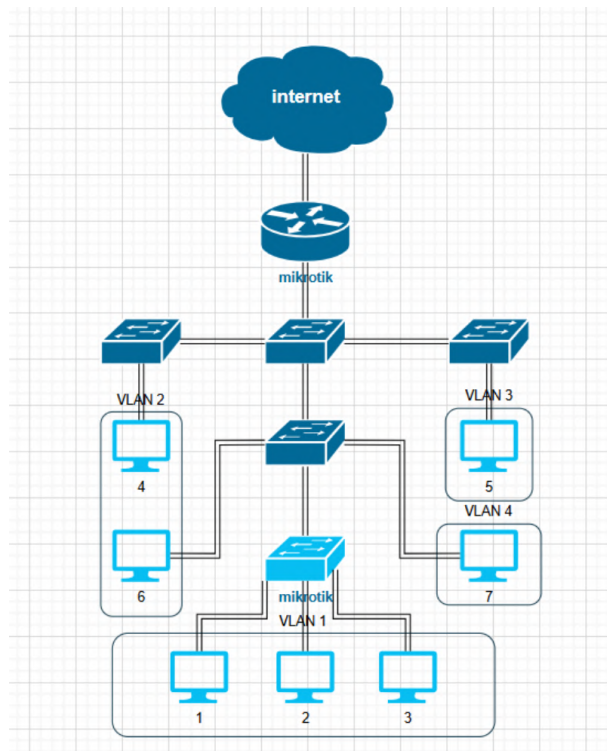


Рисунок 1 — Топология сети (вариант 7)

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).

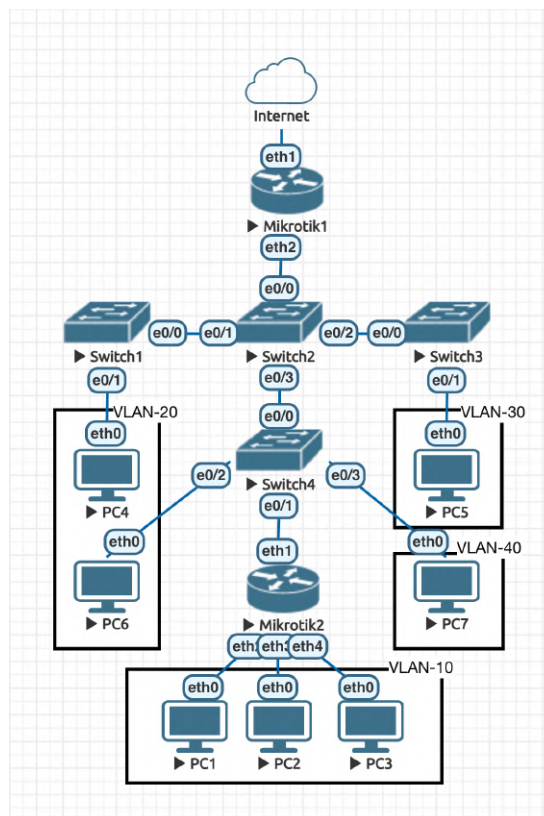


Рисунок 2 — Составленная модель сети

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).

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#hostname Switch2
Switch2(config)#vlan 10
Switch2(config-vlan)#name VLAN-10
Switch2(config-vlan)#vlan 20
Switch2(config-vlan)#name VLAN-20
Switch2(config-vlan)#vlan 30
Switch2(config-vlan)#name VLAN-30
Switch2(config-vlan)#vlan 40
Switch2(config-vlan)#name VLAN-40
Switch2(config-vlan)#do sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et1/0, Et1/1, Et1/2 Et1/3
10	VLAN-10	active	
20	VLAN-20	active	

Рисунок 3 — Добавление VLAN на Switch2

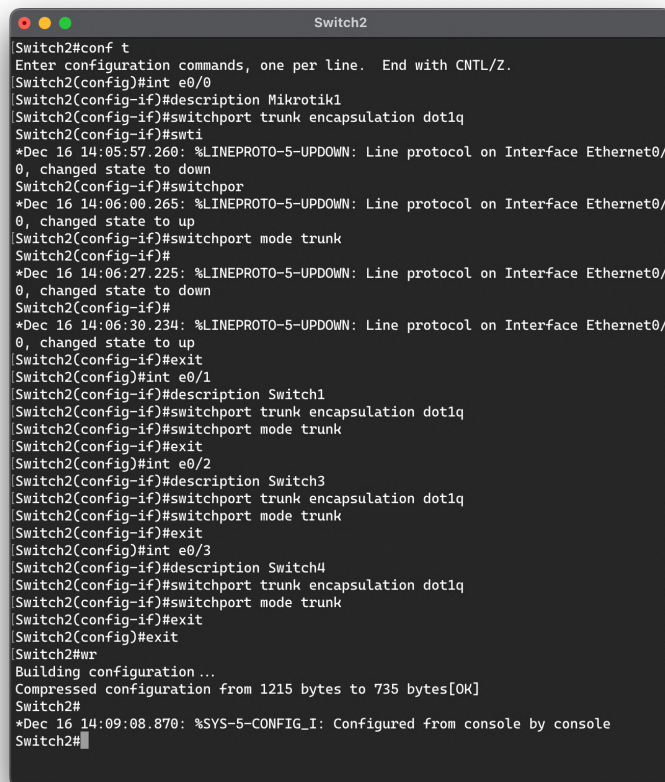
```
Switch2
```

VLAN	Name	Status	Ports
1	default	active	Et0/0, Et1/0, Et1/1, Et1/2 Et1/3
10	VLAN-10	active	
20	VLAN-20	active	
30	VLAN-30	active	
40	VLAN-40	active	
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdiinet-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
10	enet	100010	1500	-	-	-	-	-	0	0

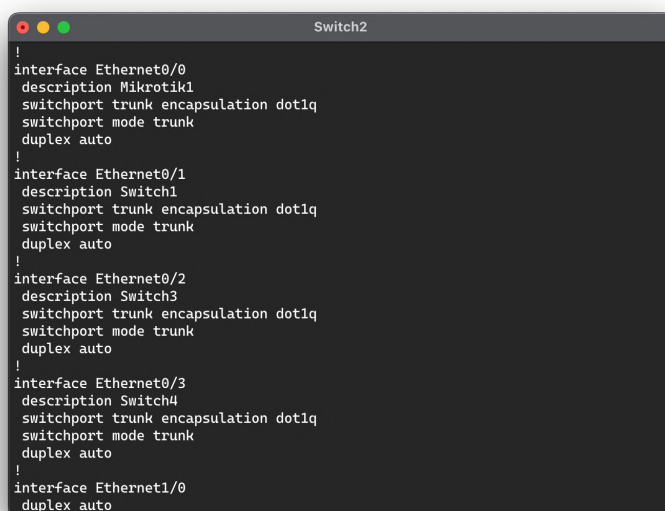
Рисунок 4 — Вывод конфигурации VLAN на Switch2

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).



```
Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#int e0/0
Switch2(config-if)#description Mikrotik1
Switch2(config-if)#switchport trunk encapsulation dot1q
Switch2(config-if)#swt
*Dec 16 14:05:57.260: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
Switch2(config-if)#switchpor
*Dec 16 14:06:00.265: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#
*Dec 16 14:06:27.225: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to down
Switch2(config-if)#
*Dec 16 14:06:30.234: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/
0, changed state to up
Switch2(config-if)#exit
Switch2(config)#int e0/1
Switch2(config-if)#description Switch1
Switch2(config-if)#switchport trunk encapsulation dot1q
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
Switch2(config)#int e0/2
Switch2(config-if)#description Switch3
Switch2(config-if)#switchport trunk encapsulation dot1q
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
Switch2(config)#int e0/3
Switch2(config-if)#description Switch4
Switch2(config-if)#switchport trunk encapsulation dot1q
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
Switch2(config)#exit
Switch2#wr
Building configuration ...
Compressed configuration from 1215 bytes to 735 bytes[OK]
Switch2#
*Dec 16 14:09:08.870: %SYS-5-CONFIG_I: Configured from console by console
Switch2#
```

Рисунок 5 — Настройка портов на Switch2



```
Switch2#
!
interface Ethernet0/0
 description Mikrotik1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/1
 description Switch1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/2
 description Switch3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet0/3
 description Switch4
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
!
interface Ethernet1/0
 duplex auto
```

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).


```
Switch2
Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#vtp domain grigorijtomczuk.local
Changing VTP domain name from NULL to grigorijtomczuk.local
Switch2(config)#
*Dec 16 14:14:15.920: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to
grigorijtomczuk.local.
Switch2(config)#vtp version 3
Switch2(config)#
*Dec 16 14:14:41.326: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN config
uration file detected and read OK. Version 3
files will be written in the future.
Switch2(config)#vtp password eve
Setting device VTP password to eve
Switch2(config)#vtp mode server
Device mode already VTP Server for VLANs.
Switch2(config)#exit
Switch2#wr
*Dec 16 14:15:50.076: %SYS-5-CONFIG_I: Configured from console by console
Switch2#
Building configuration...
Compressed configuration from 1215 bytes to 735 bytes[OK]
```

Рисунок 7 — Настройка VTP-сервера на Switch2

```
Switch2
Switch2#vtp primary
This system is becoming primary server for feature vlan
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
Switch2#
*Dec 16 14:18:15.838: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.b000 has beco
me the primary server for the VLAN VTP feature
Switch2#sh vtp status
VTP Version capable      : 1 to 3
VTP version running      : 3
VTP Domain Name         : grigorijtomczuk.local
VTP Pruning Mode        : Disabled
VTP Traps Generation     : Disabled
Device ID               : aabb.cc00.b000

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   : 1
```

Рисунок 8 — Вывод конфигурации VTP-сервера на Switch2

```
Switch1
Switch>ena
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vtp version 3
Switch(config)#
*Dec 16 14:21:06.915: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN config
uration file detected and read OK. Version 3
files will be written in the future.
Switch(config)#vtp password eve
Setting device VTP password to eve
Switch(config)#vtp mode client
Setting device to VTP Client mode for VLANs.
Switch(config)#exit
Switch#wr
*Dec 16 14:21:34.605: %SYS-5-CONFIG_I: Configured from console by console
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#hostname Switch1
Switch1(config)#exit
Switch1#wr
Building configuration...
Compressed configuration from 885 bytes to 574 bytes[OK]
Switch1#
*Dec 16 14:21:46.678: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 9 — Настройка VTP-клиента на Switch1

```

Switch1
Switch1#sh vtp status
VTP Version capable      : 1 to 3
VTP version running      : 3
VTP Domain Name          : grigorijtomczuk.local
VTP Pruning Mode         : Disabled
VTP Traps Generation     : Disabled
Device ID                : aabb.cc00.a000

Feature VLAN:
VTP Operating Mode       : Client
Number of existing VLANs : 9
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision   : 1
Primary ID               : aabb.cc00.b000
Primary Description      : Switch2
MD5 digest               : 0xFE 0xA1 0xE6 0x35 0x63 0x4A 0x56 0x92
                        : 0x45 0x46 0x16 0x1A 0x51 0xD5 0x58 0x2A

Feature MST:
VTP Operating Mode       : Transparent

```

Рисунок 10 — Вывод конфигурации VTP-клиента на Switch1

```

Switch1
Switch1#sh vlan

```

VLAN	Name	Status	Ports
1	default	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3
10	VLAN-10	active	
20	VLAN-20	active	
30	VLAN-30	active	
40	VLAN-40	active	
1002	fdi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fdinet-default	act/unsup	
1005	trbrf-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0

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).

```

Switch1
Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch1(config)#int e0/0
Switch1(config-if)#description Switch2
Switch1(config-if)#switchport trunk encapsulation dot1q
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit
Switch1(config)#int e0/1
Switch1(config-if)#description PC4
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#exit
Switch1(config)#exit
Switch1#
Building configuration...
Compressed configuration from 1035 bytes to 665 bytes[OK]
Switch1#
*Dec 16 14:34:13.778: %SYS-5-CONFIG_I: Configured from console by console

```

Рисунок 12 — Настройка портов на Switch1

```

Switch1
!
!
!
interface Ethernet0/0
description Switch2
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/1
description PC4
switchport access vlan 20
switchport mode access
duplex auto
!
interface Ethernet0/2
duplex auto
!

```

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.

```

Switch4
!
interface Ethernet0/0
description Switch2
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/1
description Mikrotik2
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
!
interface Ethernet0/2
description PC6
switchport access vlan 20
switchport mode access
duplex auto
!
interface Ethernet0/3
description PC7
switchport access vlan 40
switchport mode access
duplex auto
!

```

Рисунок 14 — Вывод конфигурации портов на Switch4

Switch4

```
Switch4#sh vlan
```

VLAN	Name	Status	Ports
1	default	active	Et1/0, Et1/1, Et1/2, Et1/3
10	VLAN-10	active	
20	VLAN-20	active	Et0/2
30	VLAN-30	active	
40	VLAN-40	active	Et0/3
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

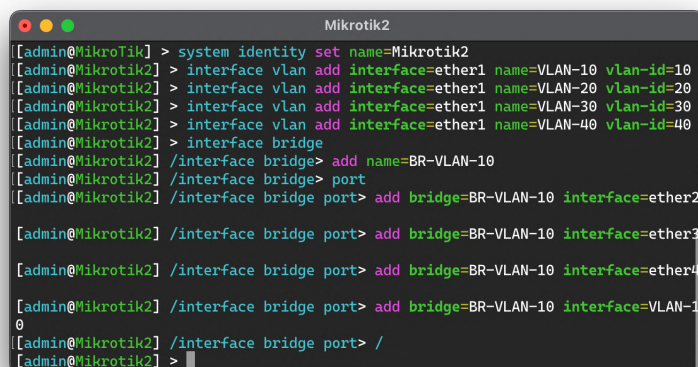
VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0

Рисунок 15 — Вывод конфигурации VLAN на Switch4

2.4 Настройка маршрутизаторов Mikrotik

Сперва был настроен маршрутизатор Mikrotik2. Вручную были

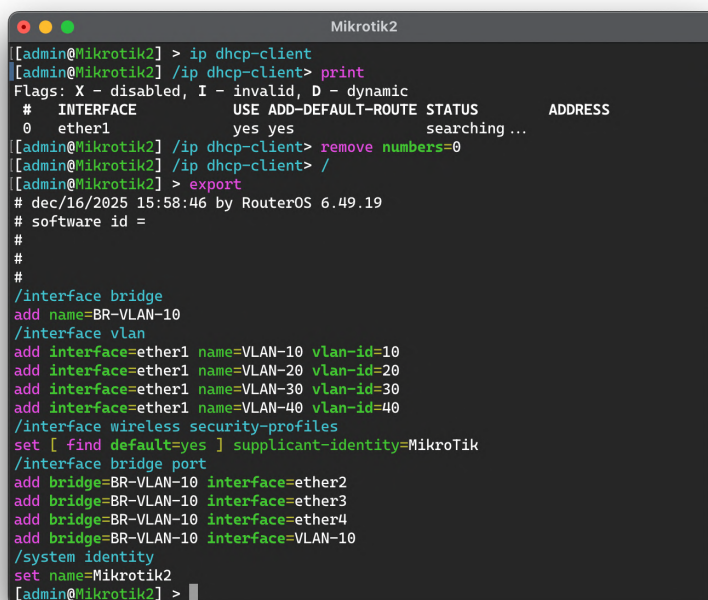
добавлены все ранее созданные VLAN, а затем был создан мост между интерфейсом VLAN-10 и соответствующими портами маршрутизатора (eth2, eth3, eth4) (рисунок 16).



```
[admin@Mikrotik] > system identity set name=Mikrotik2
[admin@Mikrotik2] > interface vlan add interface=ether1 name=VLAN-10 vlan-id=10
[admin@Mikrotik2] > interface vlan add interface=ether1 name=VLAN-20 vlan-id=20
[admin@Mikrotik2] > interface vlan add interface=ether1 name=VLAN-30 vlan-id=30
[admin@Mikrotik2] > interface vlan add interface=ether1 name=VLAN-40 vlan-id=40
[admin@Mikrotik2] > interface bridge
[admin@Mikrotik2] /interface bridge> add name=BR-VLAN-10
[admin@Mikrotik2] /interface bridge> port
[admin@Mikrotik2] /interface bridge port> add bridge=BR-VLAN-10 interface=ether2
[admin@Mikrotik2] /interface bridge port> add bridge=BR-VLAN-10 interface=ether3
[admin@Mikrotik2] /interface bridge port> add bridge=BR-VLAN-10 interface=ether4
[admin@Mikrotik2] /interface bridge port> add bridge=BR-VLAN-10 interface=VLAN-10
[admin@Mikrotik2] /interface bridge port> /
[admin@Mikrotik2] >
```

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

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

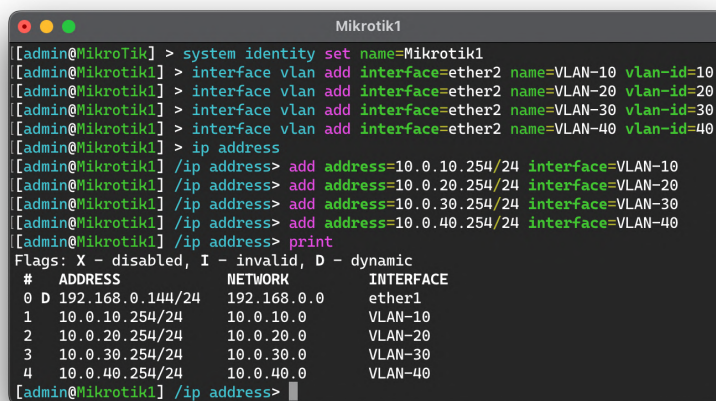


```
[admin@Mikrotik2] > ip dhcp-client
[admin@Mikrotik2] /ip dhcp-client> print
Flags: X - disabled, I - invalid, D - dynamic
# INTERFACE USE ADD-DEFAULT-ROUTE STATUS ADDRESS
0 ether1 yes yes searching ...
[admin@Mikrotik2] /ip dhcp-client> remove numbers=0
[admin@Mikrotik2] /ip dhcp-client> /
[admin@Mikrotik2] > export
# dec/16/2025 15:58:46 by RouterOS 6.49.19
# software id =
#
#
#
/interface bridge
add name=BR-VLAN-10
/interface vlan
add interface=ether1 name=VLAN-10 vlan-id=10
add interface=ether1 name=VLAN-20 vlan-id=20
add interface=ether1 name=VLAN-30 vlan-id=30
add interface=ether1 name=VLAN-40 vlan-id=40
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=BR-VLAN-10 interface=ether2
add bridge=BR-VLAN-10 interface=ether3
add bridge=BR-VLAN-10 interface=ether4
add bridge=BR-VLAN-10 interface=VLAN-10
/system identity
set name=Mikrotik2
[admin@Mikrotik2] >
```

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

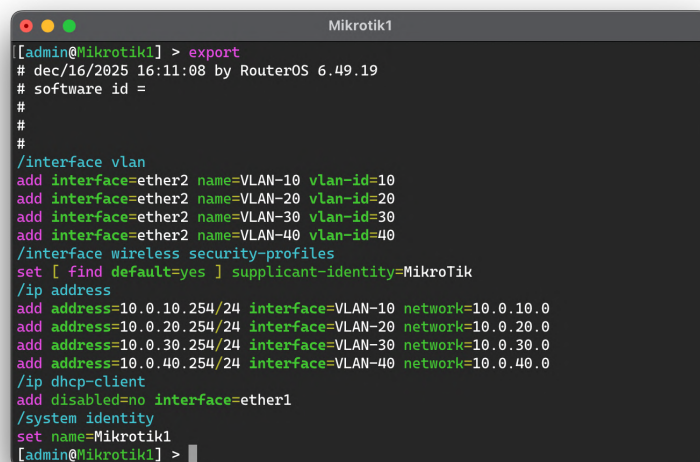
Далее был настроен маршрутизатор Mikrotik1. Он должен выполнять роль DHCP-сервера, объединяющего все VLAN и предоставляющего

доступ в интернет (рисунки 18–19).



```
Mikrotik1
[admin@Mikrotik1] > system identity set name=Mikrotik1
[admin@Mikrotik1] > interface vlan add interface=ether2 name=VLAN-10 vlan-id=10
[admin@Mikrotik1] > interface vlan add interface=ether2 name=VLAN-20 vlan-id=20
[admin@Mikrotik1] > interface vlan add interface=ether2 name=VLAN-30 vlan-id=30
[admin@Mikrotik1] > interface vlan add interface=ether2 name=VLAN-40 vlan-id=40
[admin@Mikrotik1] > ip address
[admin@Mikrotik1] /ip address> add address=10.0.10.254/24 interface=VLAN-10
[admin@Mikrotik1] /ip address> add address=10.0.20.254/24 interface=VLAN-20
[admin@Mikrotik1] /ip address> add address=10.0.30.254/24 interface=VLAN-30
[admin@Mikrotik1] /ip address> add address=10.0.40.254/24 interface=VLAN-40
[admin@Mikrotik1] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 D 192.168.0.144/24 192.168.0.0 ether1
1 10.0.10.254/24 10.0.10.0 VLAN-10
2 10.0.20.254/24 10.0.20.0 VLAN-20
3 10.0.30.254/24 10.0.30.0 VLAN-30
4 10.0.40.254/24 10.0.40.0 VLAN-40
[admin@Mikrotik1] /ip address>
```

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



```
Mikrotik1
[admin@Mikrotik1] > export
# dec/16/2025 16:11:08 by RouterOS 6.49.19
# software id =
#
#
#
/interface vlan
add interface=ether2 name=VLAN-10 vlan-id=10
add interface=ether2 name=VLAN-20 vlan-id=20
add interface=ether2 name=VLAN-30 vlan-id=30
add interface=ether2 name=VLAN-40 vlan-id=40
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip address
add address=10.0.10.254/24 interface=VLAN-10 network=10.0.10.0
add address=10.0.20.254/24 interface=VLAN-20 network=10.0.20.0
add address=10.0.30.254/24 interface=VLAN-30 network=10.0.30.0
add address=10.0.40.254/24 interface=VLAN-40 network=10.0.40.0
/ip dhcp-client
add disabled=no interface=ether1
/system identity
set name=Mikrotik1
[admin@Mikrotik1] >
```

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).

```

Mikrotik1
[admin@Mikrotik1] > ip dhcp-client print
Flags: X - disabled, I - invalid, D - dynamic
# INTERFACE USE ADD-DEFAULT-ROUTE STATUS ADDRESS
0 ether1 yes yes bound 192.168.0.144/24
[admin@Mikrotik1] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK INTERFACE
0 10.0.10.254/24 10.0.10.0 VLAN-10
1 10.0.20.254/24 10.0.20.0 VLAN-20
2 10.0.30.254/24 10.0.30.0 VLAN-30
3 10.0.40.254/24 10.0.40.0 VLAN-40
4 D 192.168.0.144/24 192.168.0.0 ether1
[admin@Mikrotik1] >

```

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).

4

IP Pool

Pools

Used Addresses

New

Remove

Find

Filter

<div><input type="checkbox"/></div>	Name	Addresses	Next Pool
<div><input type="checkbox"/></div>	<div><div></div>VLAN-10</div>	10.0.10.1 - 10.0.10.100	none
<div><input type="checkbox"/></div>	<div><div></div>VLAN-20</div>	10.0.20.1 - 10.0.20.100	none
<div><input type="checkbox"/></div>	<div><div></div>VLAN-30</div>	10.0.30.1 - 10.0.30.100	none
<div><input type="checkbox"/></div>	<div><div></div>VLAN-40</div>	10.0.40.1 - 10.0.40.100	none

4

Live

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

v4 DHCP Server						
DHCP						
New Enable Disable Remove Find Filter						
	Name	Interface	Relay	Lease Time	Address Pool	
<input type="checkbox"/>	DHCP-VLAN-10	VLAN-10		00:10:00	VLAN-10	
<input type="checkbox"/>	DHCP-VLAN-20	VLAN-20		00:10:00	VLAN-20	
<input type="checkbox"/>	DHCP-VLAN-30	VLAN-30		00:10:00	VLAN-30	
<input type="checkbox"/>	DHCP-VLAN-40	VLAN-40		00:10:00	VLAN-40	

Рисунок 23 — Настройка DHCP-серверов на Mikrotik1

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

```

Mikrotik1
[admin@Mikrotik1] > export
# dec/16/2025 16:32:01 by RouterOS 6.49.19
# software id =
#
#
#
/interface vlan
add interface=ether2 name=VLAN-10 vlan-id=10
add interface=ether2 name=VLAN-20 vlan-id=20
add interface=ether2 name=VLAN-30 vlan-id=30
add interface=ether2 name=VLAN-40 vlan-id=40
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=VLAN-10 ranges=10.0.10.1-10.0.10.100
add name=VLAN-20 ranges=10.0.20.1-10.0.20.100
add name=VLAN-30 ranges=10.0.30.1-10.0.30.100
add name=VLAN-40 ranges=10.0.40.1-10.0.40.100
/ip dhcp-server
add address-pool=VLAN-10 disabled=no interface=VLAN-10 name=DHCP-VLAN-10
add address-pool=VLAN-20 disabled=no interface=VLAN-20 name=DHCP-VLAN-20
add address-pool=VLAN-30 disabled=no interface=VLAN-30 name=DHCP-VLAN-30
add address-pool=VLAN-40 disabled=no interface=VLAN-40 name=DHCP-VLAN-40
/ip address
add address=10.0.10.254/24 interface=VLAN-10 network=10.0.10.0
add address=10.0.20.254/24 interface=VLAN-20 network=10.0.20.0
add address=10.0.30.254/24 interface=VLAN-30 network=10.0.30.0
add address=10.0.40.254/24 interface=VLAN-40 network=10.0.40.0
/ip dhcp-client
add disabled=no interface=ether1
/ip dhcp-server network
add address=10.0.10.0/24 dns-server=8.8.8.8 gateway=10.0.10.254
add address=10.0.20.0/24 dns-server=8.8.8.8 gateway=10.0.20.254
add address=10.0.30.0/24 dns-server=8.8.8.8 gateway=10.0.30.254
add address=10.0.40.0/24 dns-server=8.8.8.8 gateway=10.0.40.254
/system identity
set name=Mikrotik1
[admin@Mikrotik1] >

```

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).

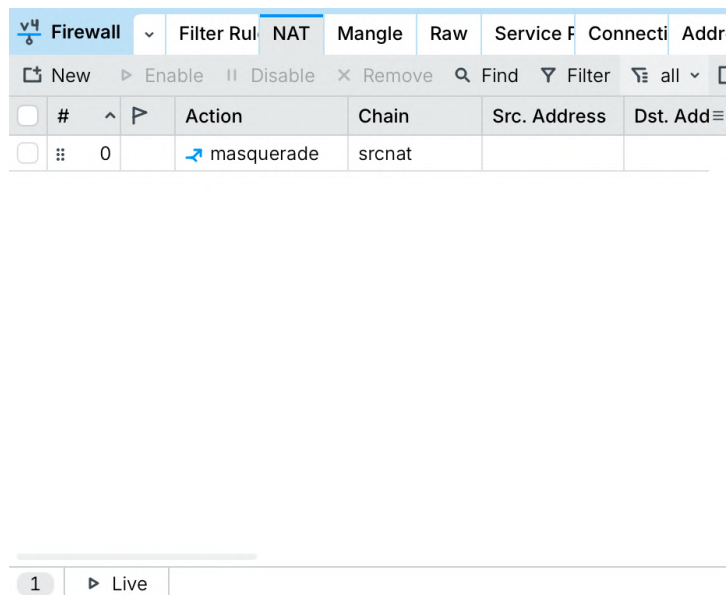


Рисунок 25 — Добавленное NAT-правило на Mikrotik1

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).

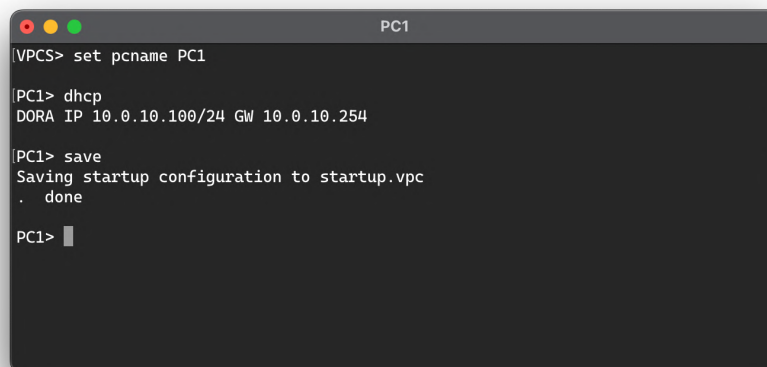


Рисунок 26 — Настройка PC1

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


```
PC6> show ip

NAME       : PC6[1]
IP/MASK    : 10.0.20.99/24
GATEWAY    : 10.0.20.254
DNS        : 8.8.8.8
DHCP SERVER: 10.0.20.254
DHCP LEASE : 433, 600/300/525
MAC        : 00:50:79:66:68:06
LPORT      : 20000
RHOST:PORT : 127.0.0.1:30000
MTU        : 1500

PC6>

PC4> ping 10.0.20.99

84 bytes from 10.0.20.99 icmp_seq=1 ttl=64 time=0.888 ms
84 bytes from 10.0.20.99 icmp_seq=2 ttl=64 time=1.324 ms
84 bytes from 10.0.20.99 icmp_seq=3 ttl=64 time=1.323 ms
^C
PC4>
```

Рисунок 27 — Проверка связи внутри VLAN-20

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

```
PC3> show ip

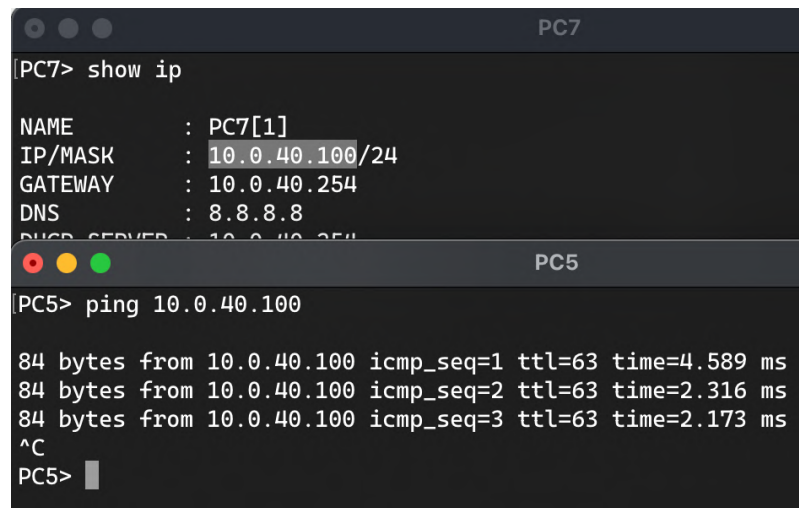
NAME       : PC3[1]
IP/MASK    : 10.0.10.98/24
GATEWAY    : 10.0.10.254
DNS        : 8.8.8.8

PC1> ping 10.0.10.98

84 bytes from 10.0.10.98 icmp_seq=1 ttl=64 time=0.643 ms
84 bytes from 10.0.10.98 icmp_seq=2 ttl=64 time=0.804 ms
84 bytes from 10.0.10.98 icmp_seq=3 ttl=64 time=0.867 ms
^C
PC1>
```

Рисунок 28 — Проверка связи внутри VLAN-10

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



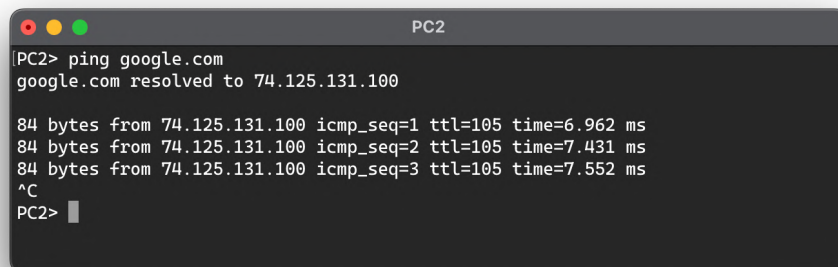
The image shows two overlapping terminal windows. The top window, titled 'PC7', displays the output of the 'show ip' command, showing the IP address 10.0.40.100/24 and gateway 10.0.40.254. The bottom window, titled 'PC5', shows the output of a 'ping 10.0.40.100' command, displaying three successful ping attempts with times around 2-5 ms.

```
PC7> show ip
NAME       : PC7[1]
IP/MASK    : 10.0.40.100/24
GATEWAY    : 10.0.40.254
DNS        : 8.8.8.8
DHCP SERVER: 10.0.40.254

PC5> ping 10.0.40.100
84 bytes from 10.0.40.100 icmp_seq=1 ttl=63 time=4.589 ms
84 bytes from 10.0.40.100 icmp_seq=2 ttl=63 time=2.316 ms
84 bytes from 10.0.40.100 icmp_seq=3 ttl=63 time=2.173 ms
^C
PC5>
```

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).

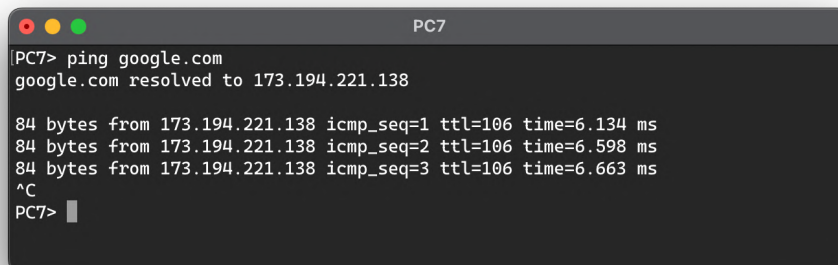


The image shows a terminal window titled 'PC2'. It displays the output of a 'ping google.com' command, showing the IP address 74.125.131.100 and three successful ping attempts with times around 6-8 ms.

```
PC2> ping google.com
google.com resolved to 74.125.131.100

84 bytes from 74.125.131.100 icmp_seq=1 ttl=105 time=6.962 ms
84 bytes from 74.125.131.100 icmp_seq=2 ttl=105 time=7.431 ms
84 bytes from 74.125.131.100 icmp_seq=3 ttl=105 time=7.552 ms
^C
PC2>
```

Рисунок 30 — Проверка доступа в интернет из VLAN-10



The image shows a terminal window titled 'PC7'. It displays the output of a 'ping google.com' command, showing the IP address 173.194.221.138 and three successful ping attempts with times around 6 ms.

```
PC7> ping google.com
google.com resolved to 173.194.221.138

84 bytes from 173.194.221.138 icmp_seq=1 ttl=106 time=6.134 ms
84 bytes from 173.194.221.138 icmp_seq=2 ttl=106 time=6.598 ms
84 bytes from 173.194.221.138 icmp_seq=3 ttl=106 time=6.663 ms
^C
PC7>
```

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)