

# **Отчет по лабораторной работе № 16**

**Администрирование локальных сетей**

Амуничников Антон, НПИбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>4</b>	<b>Выводы</b>	<b>17</b>
<b>5</b>	<b>Контрольные вопросы</b>	<b>18</b>

## Список иллюстраций

3.1 Медиаконвертер с модулями PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE . . . . .	7
3.2 Схема сети с дополнительными площадками . . . . .	7
3.3 Перемещение оборудования в г. Пиза . . . . .	8
3.4 Добавление г. Пиза . . . . .	8
3.5 Первоначальная настройка маршрутизатора pisa-unipi-gw-1 . . . .	9
3.6 Первоначальная настройка коммутатора pisa-unipi-sw-1 . . . . .	10
3.7 Настройка интерфейсов маршрутизатора pisa-unipi-gw-1 . . . . .	11
3.8 Настройка интерфейсов коммутатора pisa-unipi-sw-1 . . . . .	12
3.9 Проверка работоспособности соединения . . . . .	13
3.10 Настройка маршрутизатора msk-donskaya-gw-1 . . . . .	14
3.11 Настройка маршрутизатора pisa-unipi-gw-1 . . . . .	15
3.12 Проверка доступности соединения . . . . .	16

# 1 Цель работы

Получить навыки настройки VPN-туннеля через незащищённое Интернет-соединение.

## 2 Задание

1. Разместить в рабочей области проекта в соответствии с модельными предположениями оборудование для сети Университета г. Пиза.
2. В физической рабочей области проекта создать город Пиза, здание Университета г. Пиза. Переместить туда соответствующее оборудование.
3. Сделать первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза.
4. Настроить VPN на основе протокола GRE.
5. Проверить доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская».

### 3 Выполнение лабораторной работы

Виртуальная частная сеть (Virtual Private Network, VPN) — технология, обеспечивающая одно или несколько сетевых соединений поверх другой сети (например, Интернет).

Сеть Университета г. Пиза (Италия) содержит маршрутизатор Cisco 2811 pisa-ipi-gw-1, коммутатор Cisco 2950 pisa-unipi-sw-1 и оконечное устройство PC pc-unipi-1.

Разместим эти устройства в рабочей области, заменим у медиаконвертеров имеющиеся модули на PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE для подключения витой пары по технологии Fast Ethernet и оптоволокна соответственно (рис. 3.1).

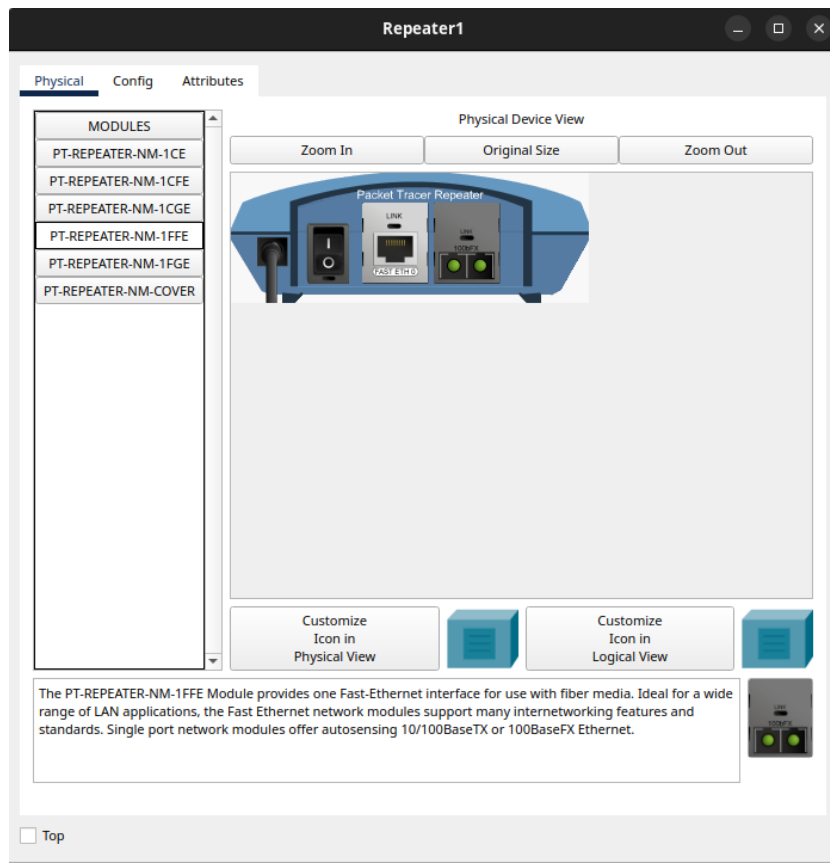


Рис. 3.1: Медиаконвертер с модулями PT-REPEATER-NM-1FFE и PT-REPEATER-NM-1CFE

Назовем устройства, выполняя соглашение об именовании, а также соединим устройства (рис. 3.2).

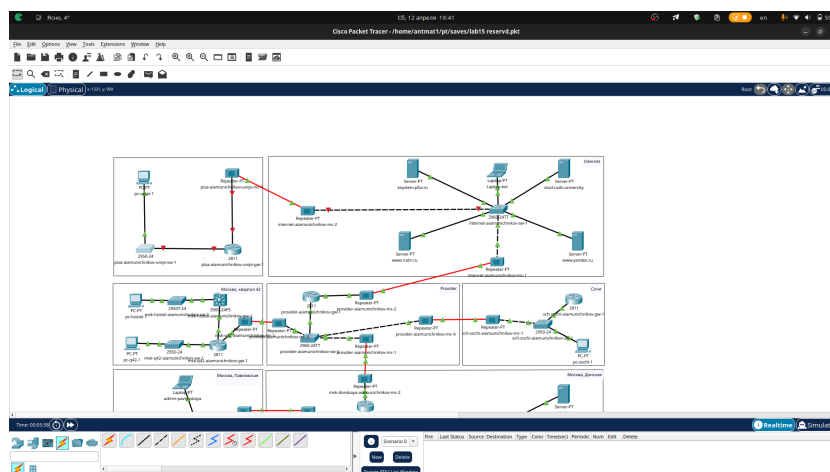


Рис. 3.2: Схема сети с дополнительными площадками

В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза и переместим туда соответствующее оборудование (рис. 3.3,3.4).

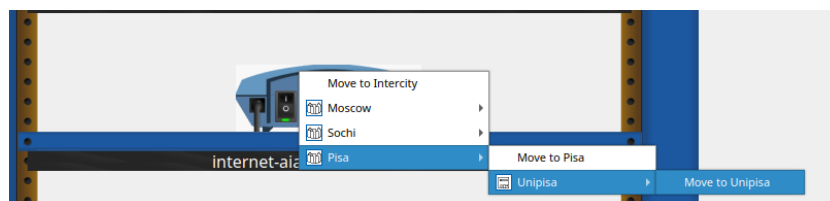


Рис. 3.3: Перемещение оборудования в г. Пиза

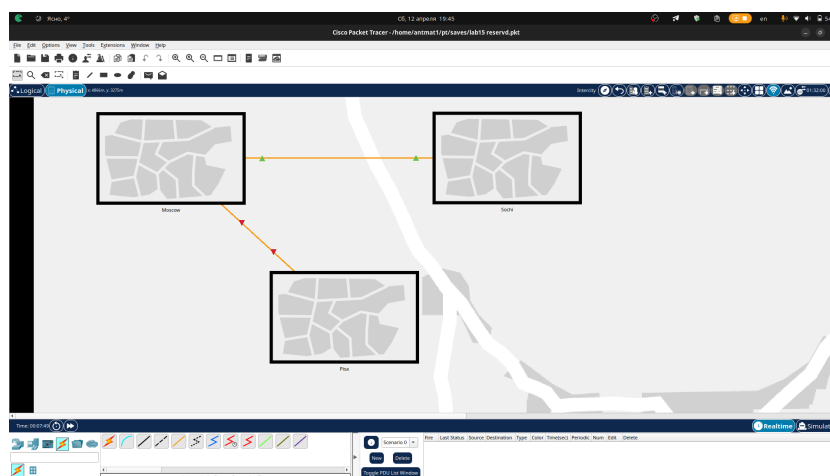


Рис. 3.4: Добавление г. Пиза

Выполним первоначальную настройку маршрутизатора pisa-unipi-gw-1 (рис. 3.5). Зададим имя, установим доступ по паролю и оставим доступ по ssh.



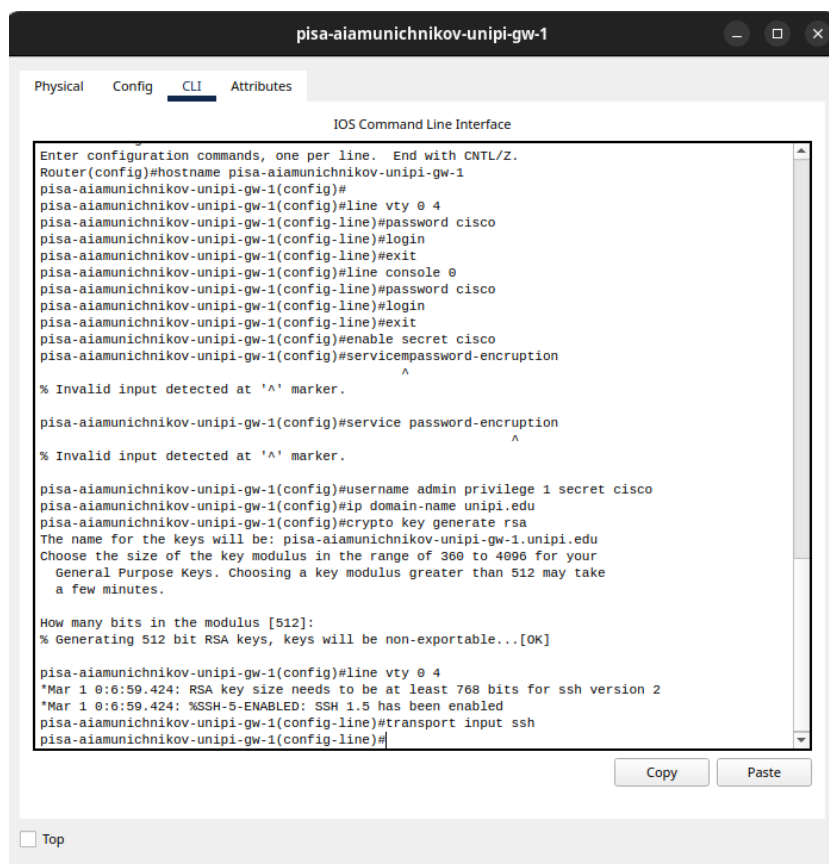
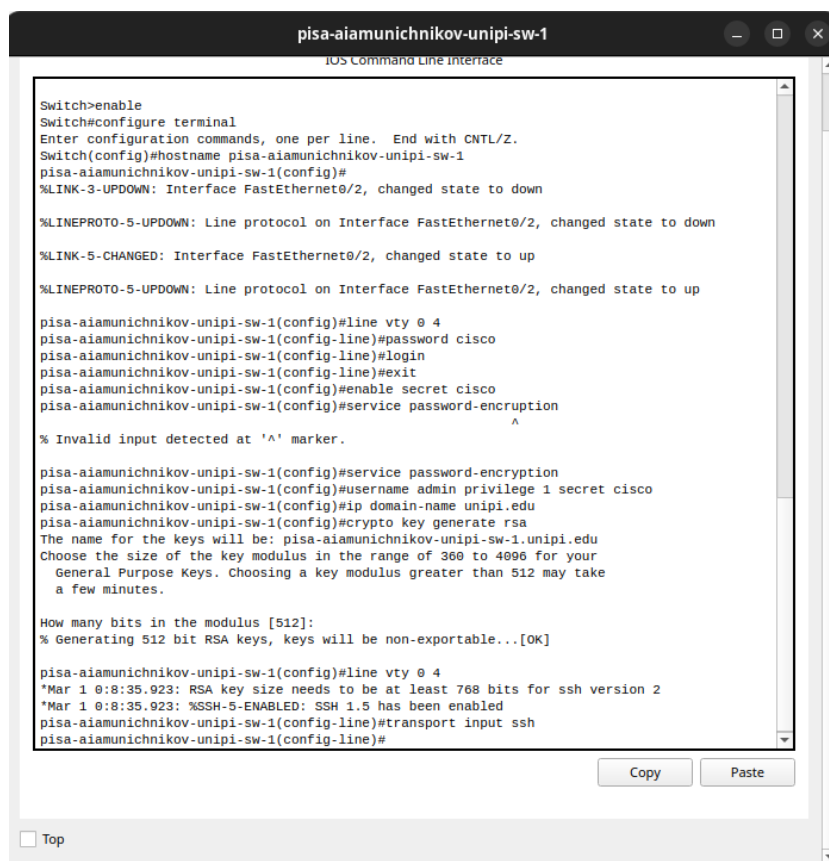


Рис. 3.5: Первоначальная настройка маршрутизатора pisa-unipi-gw-1

Выполним первоначальную настройку коммутатора pisa-unipi-sw-1 (рис. 3.6).  
Зададим имя, установим доступ по паролю и оставим доступ по ssh.



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname pisa-aiamunichnikov-unipi-sw-1
pisa-aiamunichnikov-unipi-sw-1(config)#
%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

pisa-aiamunichnikov-unipi-sw-1(config)#line vty 0 4
pisa-aiamunichnikov-unipi-sw-1(config-line)#password cisco
pisa-aiamunichnikov-unipi-sw-1(config-line)#login
pisa-aiamunichnikov-unipi-sw-1(config-line)#exit
pisa-aiamunichnikov-unipi-sw-1(config)#enable secret cisco
pisa-aiamunichnikov-unipi-sw-1(config)#service password-encryption
^
% Invalid input detected at '^' marker.

pisa-aiamunichnikov-unipi-sw-1(config)#service password-encryption
pisa-aiamunichnikov-unipi-sw-1(config)#username admin privilege 1 secret cisco
pisa-aiamunichnikov-unipi-sw-1(config)#ip domain-name unipi.edu
pisa-aiamunichnikov-unipi-sw-1(config)#crypto key generate rsa
The name for the keys will be: pisa-aiamunichnikov-unipi-sw-1.unipi.edu
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

pisa-aiamunichnikov-unipi-sw-1(config)#line vty 0 4
*Mar 1 0:8:35.923: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:8:35.923: %SSH-5-ENABLED: SSH 1.5 has been enabled
pisa-aiamunichnikov-unipi-sw-1(config-line)#transport input ssh
pisa-aiamunichnikov-unipi-sw-1(config-line)#
```

Рис. 3.6: Первоначальная настройка коммутатора pisa-unipi-sw-1

Выполним настройку интерфейсов маршрутизатора pisa-unipi-gw-1 (рис. 3.7).

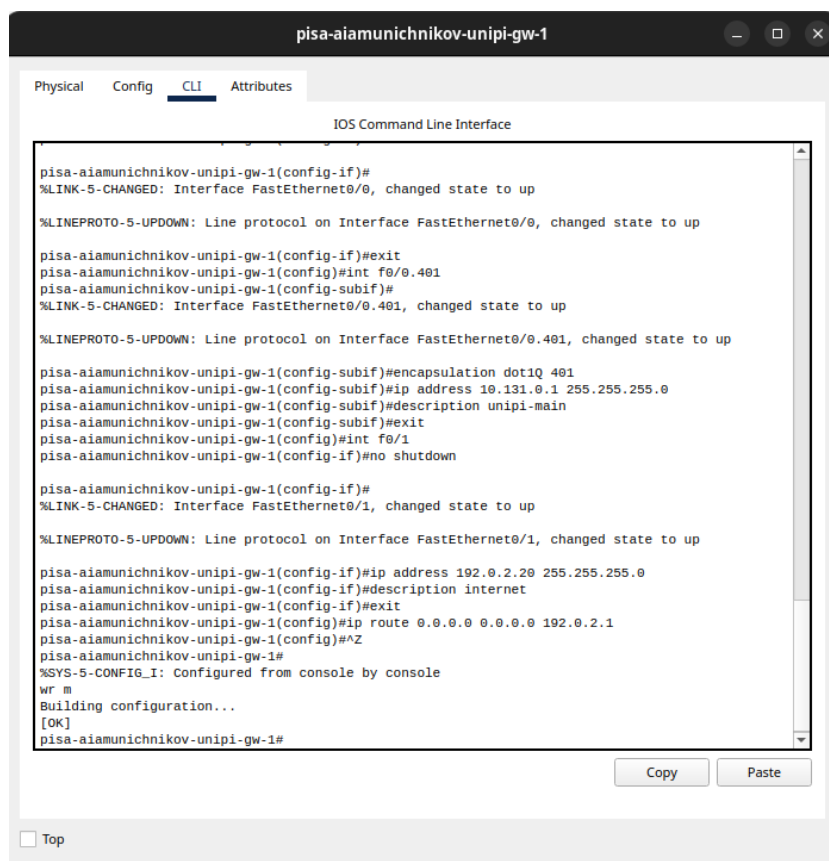


Рис. 3.7: Настройка интерфейсов маршрутизатора pisa-unipi-gw-1

Выполним настройку интерфейсов коммутатора pisa-unipi-sw-1 (рис. 3.8).

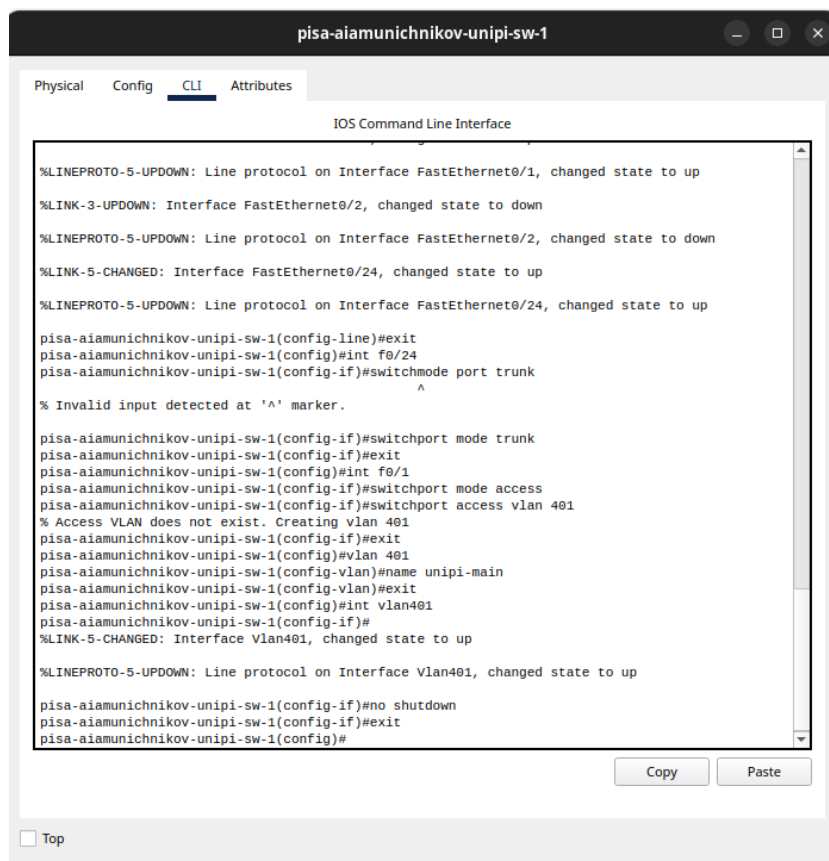


Рис. 3.8: Настройка интерфейсов коммутатора pisa-unipi-sw-1

Зададим ПК в г. Пиза ip-адрес и пропиnguем маршрутизатор, чтобы проверит работоспособность соединения (рис. 3.9). Пингование прошло успешно.

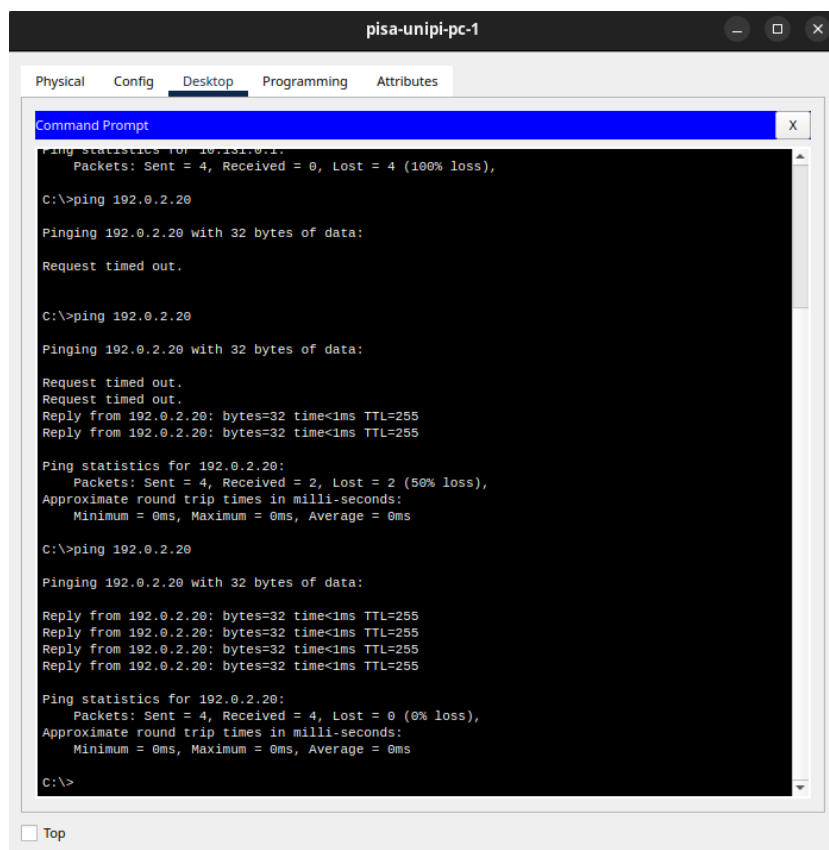


Рис. 3.9: Проверка работоспособности соединения

Выполним настройку VPN на основе GRE (рис. 3.10,3.11). Создадим интерфейс туннель, зададим ip-адрес, укажем начало и конец туннеля, также настроим интерфейс loopback.

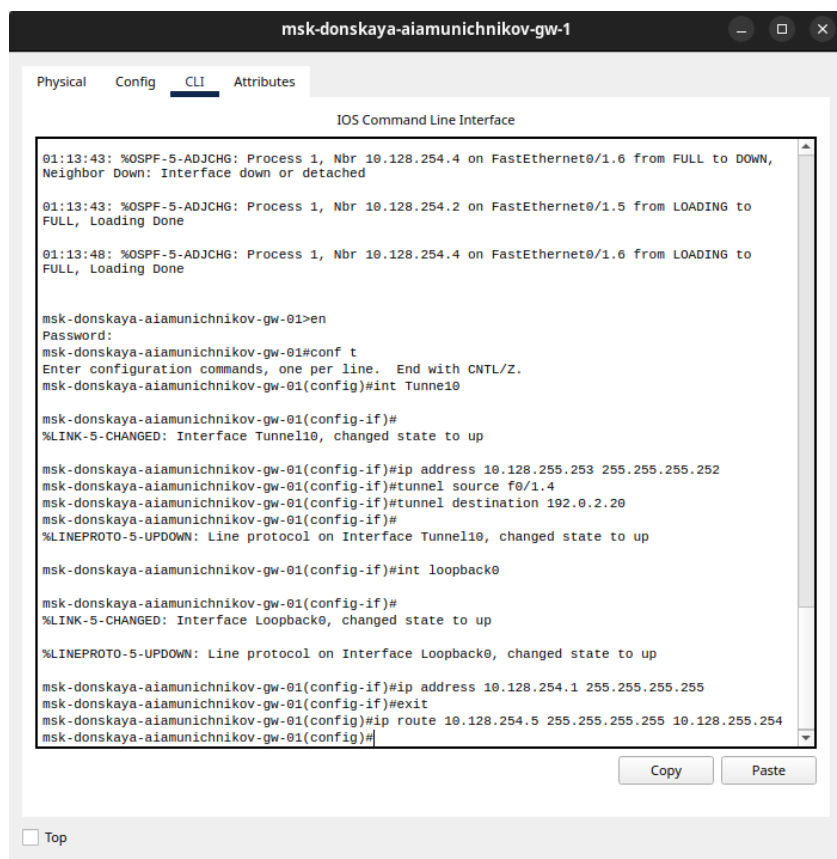


Рис. 3.10: Настройка маршрутизатора msk-donskaya-gw-1

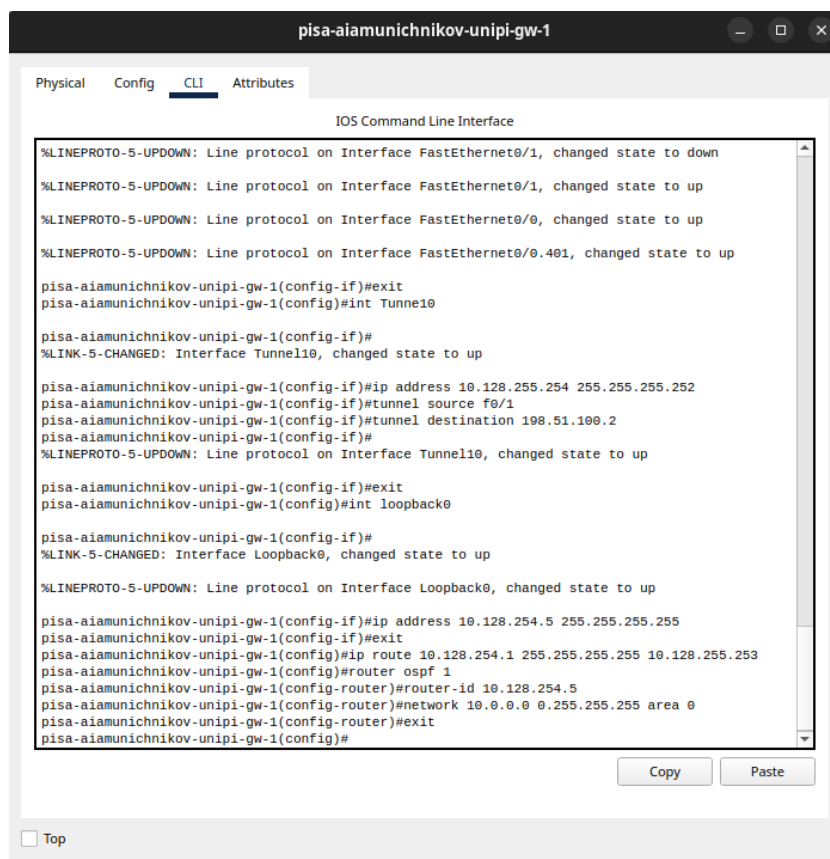


Рис. 3.11: Настройка маршрутизатора pisa-unipi-gw-1

Проверим доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская» (рис. 3.12). Пингование прошло успешно.

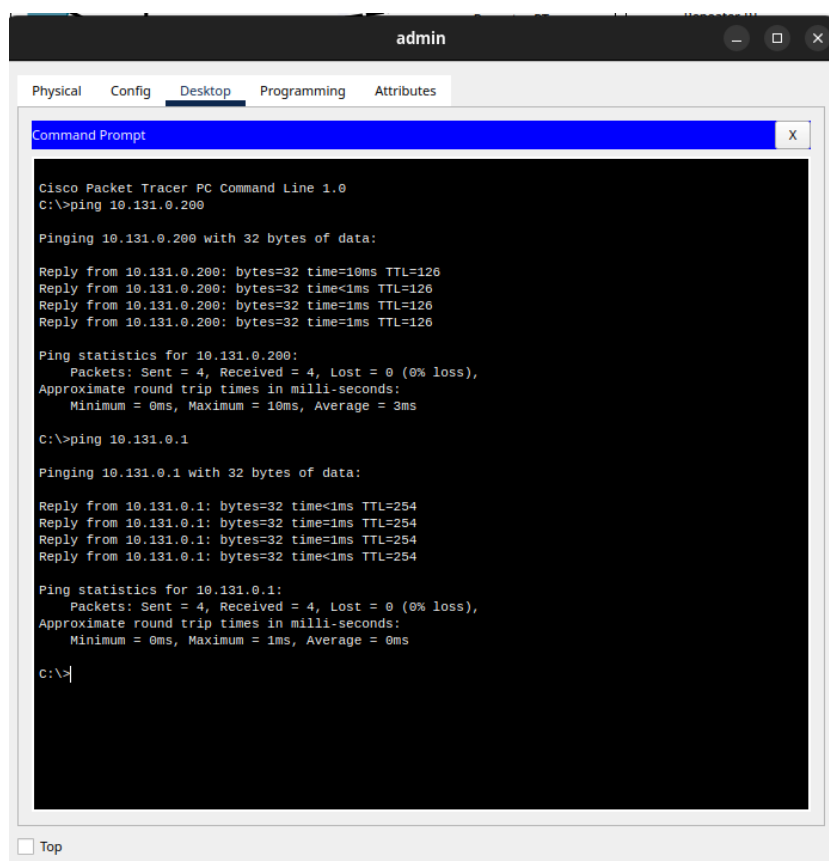


Рис. 3.12: Проверка доступности соединения



## **4 Выводы**

В результате выполнения данной лабораторной работы я получил навыки настройки VPN-туннеля через незащищённое Интернет-соединение.

## 5 Контрольные вопросы

### 1. Что такое VPN?

Виртуальная частная сеть (Virtual Private Network, VPN) — технология, обеспечивающая одно или несколько сетевых соединений поверх другой сети (например, Интернет).

### 2. В каких случаях следует использовать VPN?

VPN шифрует интернет-трафик, защищая данные от хакеров и интернет-провайдеров, что особенно важно в общедоступных Wi-Fi сетях. Он скрывает реальный IP-адрес, предотвращая отслеживание местоположения и онлайн-активности. VPN помогает обходить цензуру и географические ограничения, предоставляя доступ к заблокированным сайтам и региональному контенту. Он также незаменим для безопасной работы в корпоративных сетях, позволяя сотрудникам удаленно подключаться к корпоративным ресурсам и защищая корпоративные данные от несанкционированного доступа. VPN защищает от атак типа «человек посередине» и блокирует вредоносные веб-сайты и фишинговые атаки. Он также позволяет экономить на покупках, предоставляя доступ к региональным ценам на товары и услуги в интернете. Примеры использования VPN включают защиту личной информации в общедоступных Wi-Fi сетях, обход географических ограничений, безопасную удаленную работу и анонимный серфинг. В современном цифровом мире, где угрозы кибербезопасности и ограничения доступа становятся все более распространенными, VPN является мощным инструментом для обеспечения безопасности и конфиденциальности.

### 3. Как с помощью VPN обойти NAT?

Обход NAT с помощью VPN возможен благодаря тому, что VPN создает зашифрованное соединение между устройством пользователя и удаленным сервером, обходя при этом ограничения, налагаемые NAT. Это позволяет устройству пользователя обмениваться данными через интернет, игнорируя ограничения NAT.