Настройка VPN

Лабораторная работа № 16

Шулуужук Айраана НПИбд-02-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Получение навыков настройки VPN-туннеля через незащищённое Интернет-соединение.

2 Выполнение лабораторной работы

Разместить в рабочей области проекта в соответствии с модельными предположениями оборудование для сети Университета г. Пиза (рис. 2.1) (рис. 2.2) (рис. 2.3)

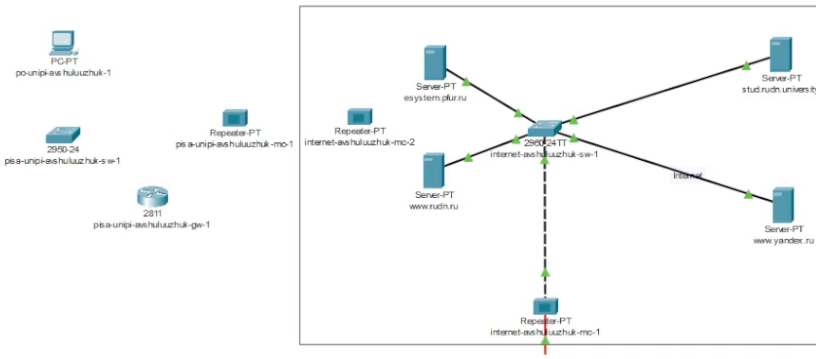


Рис. 2.1: Раземещение необходимого оборудования в сеть

Рис. 2.2: Настройка портов на медиаконвертерах

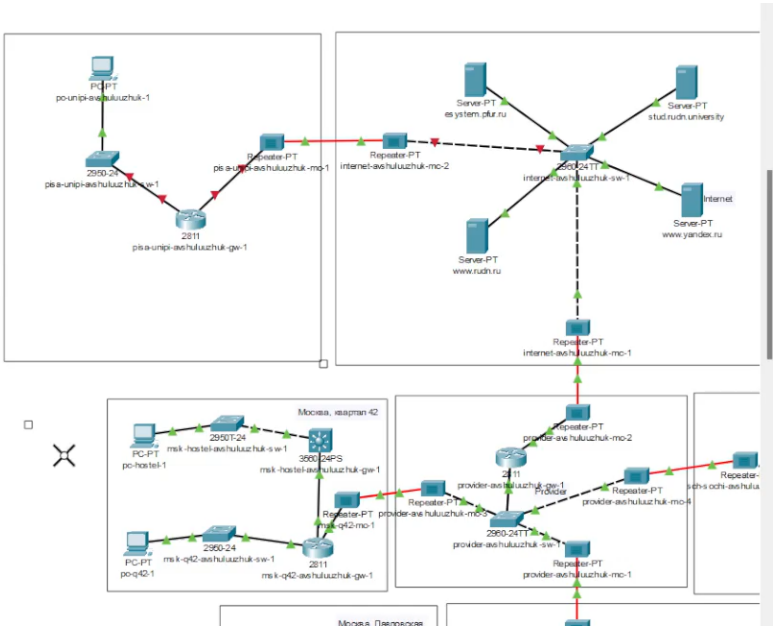


Рис. 2.3: Проведение соединеия оборудования

В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза. Переместим туда соответствующее оборудование (рис. 2.4) (рис. 2.5) (рис. 2.6)

Рис. 2.4: Создание города Пиза

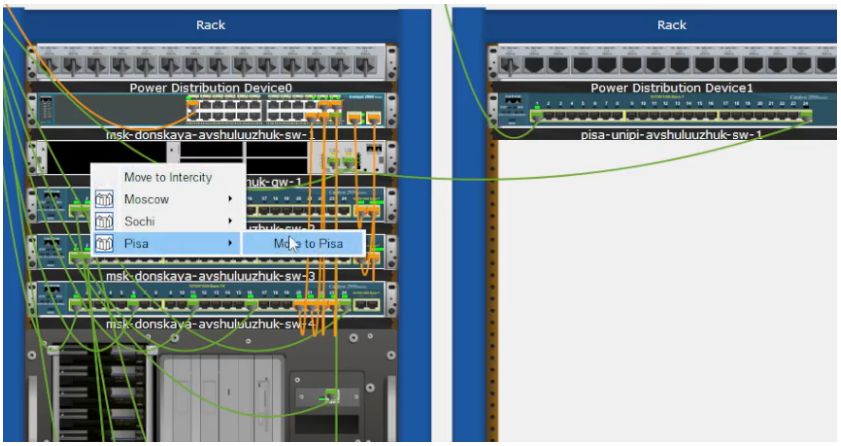


Рис. 2.5: Перемещение оборудования на соответствующие территории

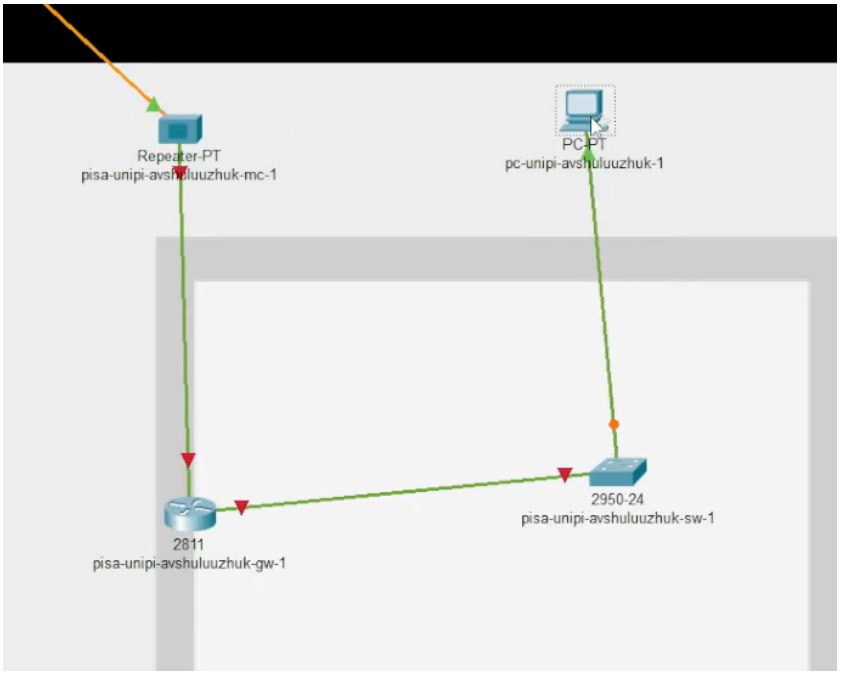
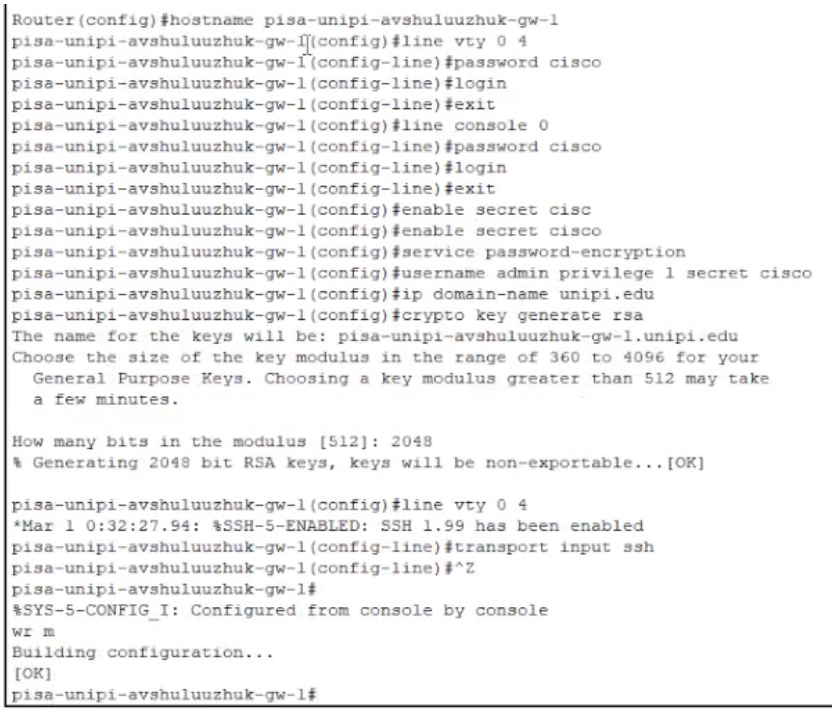


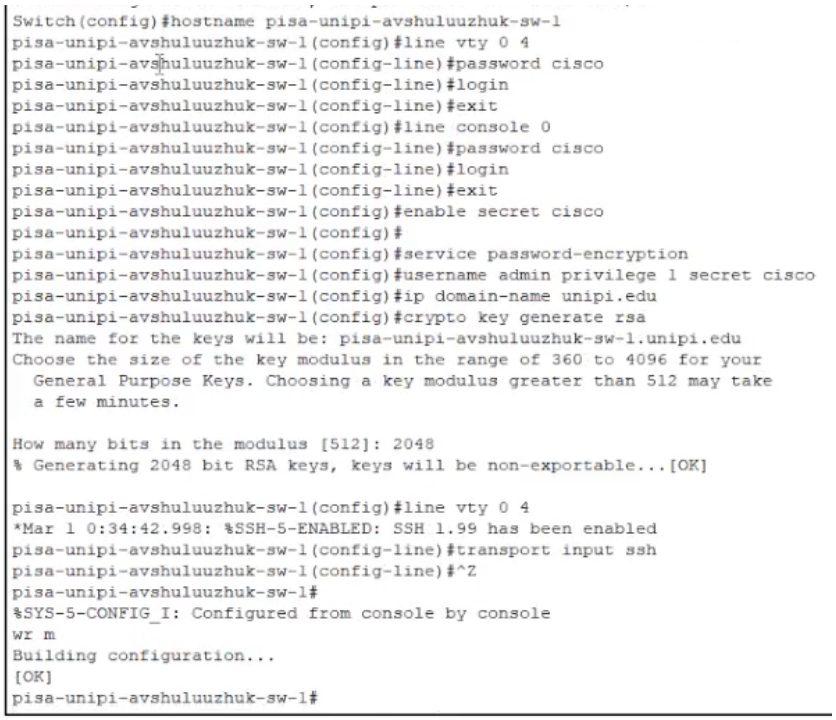
Рис. 2.6: Оборудование на территории г. Пиза

Сделаем первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза (рис. 2.7) (рис. 2.8 (рис. 2.9) (рис. 2.10)



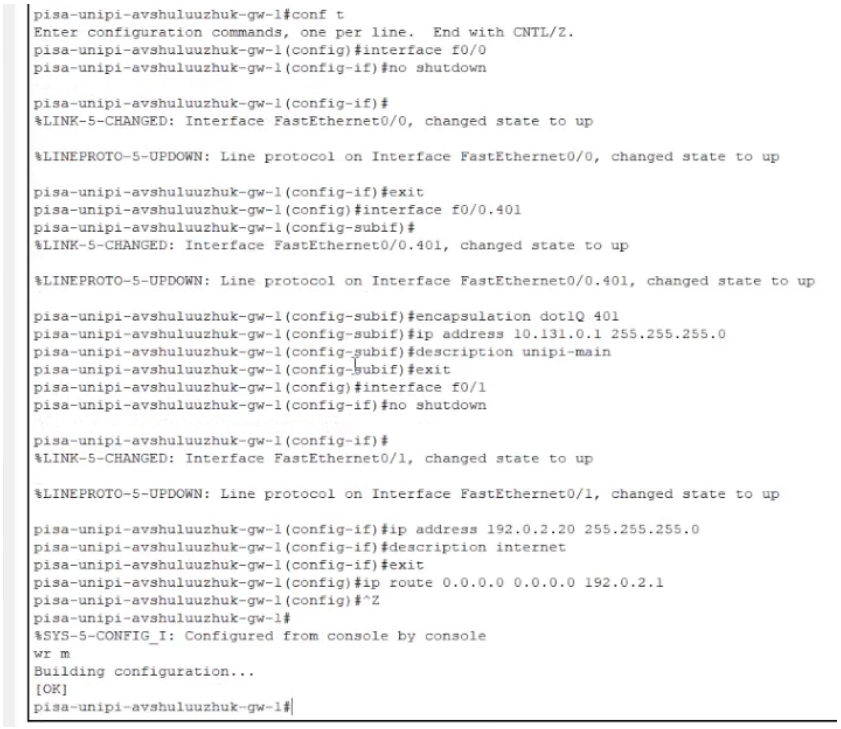
```
Router(config)#hostname pisa-unipi-avshuluuzhuk-gw-1
pisa-unipi-avshuluuzhuk-gw-1(config)#line vty 0 4
pisa-unipi-avshuluuzhuk-gw-1(config-line)#password cisco
pisa-unipi-avshuluuzhuk-gw-1(config-line)#login
pisa-unipi-avshuluuzhuk-gw-1(config-line)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#line console 0
pisa-unipi-avshuluuzhuk-gw-1(config-line)#password cisco
pisa-unipi-avshuluuzhuk-gw-1(config-line)#login
pisa-unipi-avshuluuzhuk-gw-1(config-line)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#enable secret cisc
pisa-unipi-avshuluuzhuk-gw-1(config)#enable secret cisco
pisa-unipi-avshuluuzhuk-gw-1(config)#service password-encryption
pisa-unipi-avshuluuzhuk-gw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-avshuluuzhuk-gw-1(config)#ip domain-name unipi.edu
pisa-unipi-avshuluuzhuk-gw-1(config)#crypto key generate rsa
The name for the keys will be: pisa-unipi-avshuluuzhuk-gw-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]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-avshuluuzhuk-gw-1(config)#line vty 0 4
*Mar 1 0:32:27.94: %SSH-5-ENABLED: SSH 1.99 has been enabled
pisa-unipi-avshuluuzhuk-gw-1(config-line)#transport input ssh
pisa-unipi-avshuluuzhuk-gw-1(config-line)#^Z
pisa-unipi-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
pisa-unipi-avshuluuzhuk-gw-1#
```

Рис. 2.7: Первоначальная настройка маршрутизатора pisa-unipi-gw-1



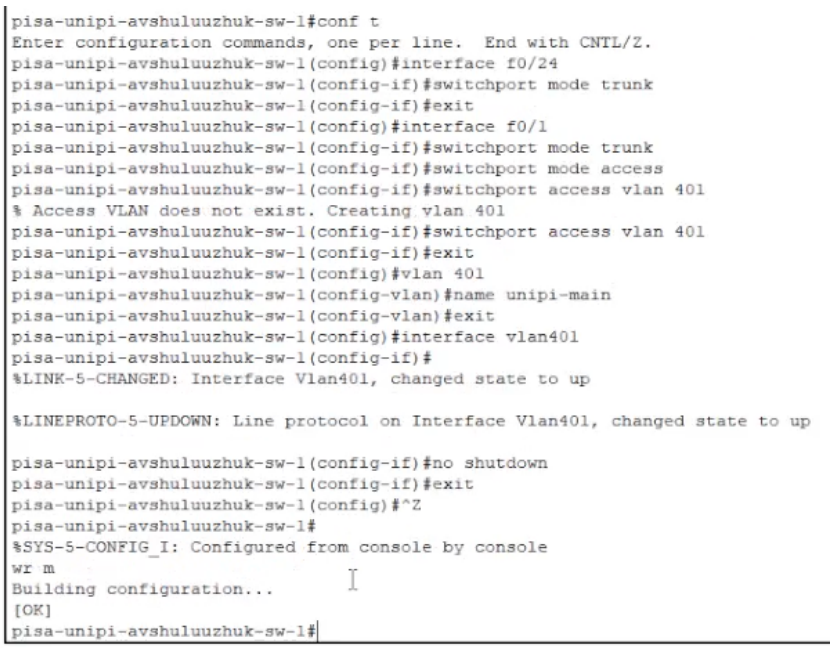
```
Switch(config)#hostname pisa-unipi-avshuluuzhuk-sw-1
pisa-unipi-avshuluuzhuk-sw-1(config)#line vty 0 4
pisa-unipi-avshuluuzhuk-sw-1(config-line)#password cisco
pisa-unipi-avshuluuzhuk-sw-1(config-line)#login
pisa-unipi-avshuluuzhuk-sw-1(config-line)#exit
pisa-unipi-avshuluuzhuk-sw-1(config)#line console 0
pisa-unipi-avshuluuzhuk-sw-1(config-line)#password cisco
pisa-unipi-avshuluuzhuk-sw-1(config-line)#login
pisa-unipi-avshuluuzhuk-sw-1(config-line)#exit
pisa-unipi-avshuluuzhuk-sw-1(config)#enable secret cisco
pisa-unipi-avshuluuzhuk-sw-1(config)#
pisa-unipi-avshuluuzhuk-sw-1(config)#service password-encryption
pisa-unipi-avshuluuzhuk-sw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-avshuluuzhuk-sw-1(config)#ip domain-name unipi.edu
pisa-unipi-avshuluuzhuk-sw-1(config)#crypto key generate rsa
The name for the keys will be: pisa-unipi-avshuluuzhuk-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]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-avshuluuzhuk-sw-1(config)#line vty 0 4
*Mar 1 0:34:42.998: %SSH-5-ENABLED: SSH 1.99 has been enabled
pisa-unipi-avshuluuzhuk-sw-1(config-line)#transport input ssh
pisa-unipi-avshuluuzhuk-sw-1(config-line)#^Z
pisa-unipi-avshuluuzhuk-sw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
pisa-unipi-avshuluuzhuk-sw-1#
```

Рис. 2.8: Первоначальная настройка коммутатора pisa-unipi-sw-1



```
pisa-unipi-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
pisa-unipi-avshuluuzhuk-gw-1(config)#interface f0/0
pisa-unipi-avshuluuzhuk-gw-1(config-if)#no shutdown

pisa-unipi-avshuluuzhuk-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

pisa-unipi-avshuluuzhuk-gw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#interface f0/0.401
pisa-unipi-avshuluuzhuk-gw-1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.401, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.401, changed state to up

pisa-unipi-avshuluuzhuk-gw-1(config-subif)#encapsulation dot1Q 401
pisa-unipi-avshuluuzhuk-gw-1(config-subif)#ip address 10.131.0.1 255.255.255.0
pisa-unipi-avshuluuzhuk-gw-1(config-subif)#description unipi-main
pisa-unipi-avshuluuzhuk-gw-1(config-subif)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#interface f0/1
pisa-unipi-avshuluuzhuk-gw-1(config-if)#no shutdown

pisa-unipi-avshuluuzhuk-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

pisa-unipi-avshuluuzhuk-gw-1(config-if)#ip address 192.0.2.20 255.255.255.0
pisa-unipi-avshuluuzhuk-gw-1(config-if)#description internet
pisa-unipi-avshuluuzhuk-gw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#ip route 0.0.0.0 0.0.0.0 192.0.2.1
pisa-unipi-avshuluuzhuk-gw-1(config)#^Z
pisa-unipi-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
pisa-unipi-avshuluuzhuk-gw-1#
```

Рис. 2.9: Настройка интерфейсов маршрутизатора pisa-unipi-gw-1



```
pisa-unipi-avshuluuzhuk-sw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
pisa-unipi-avshuluuzhuk-sw-1(config)#interface f0/24
pisa-unipi-avshuluuzhuk-sw-1(config-if)#switchport mode trunk
pisa-unipi-avshuluuzhuk-sw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-sw-1(config)#interface f0/1
pisa-unipi-avshuluuzhuk-sw-1(config-if)#switchport mode trunk
pisa-unipi-avshuluuzhuk-sw-1(config-if)#switchport mode access
pisa-unipi-avshuluuzhuk-sw-1(config-if)#switchport access vlan 401
% Access VLAN does not exist. Creating vlan 401
pisa-unipi-avshuluuzhuk-sw-1(config-if)#switchport access vlan 401
pisa-unipi-avshuluuzhuk-sw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-sw-1(config)#vlan 401
pisa-unipi-avshuluuzhuk-sw-1(config-vlan)#name unipi-main
pisa-unipi-avshuluuzhuk-sw-1(config-vlan)#exit
pisa-unipi-avshuluuzhuk-sw-1(config)#interface vlan401
pisa-unipi-avshuluuzhuk-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan401, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan401, changed state to up

pisa-unipi-avshuluuzhuk-sw-1(config-if)#no shutdown
pisa-unipi-avshuluuzhuk-sw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-sw-1(config)#^Z
pisa-unipi-avshuluuzhuk-sw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
pisa-unipi-avshuluuzhuk-sw-1#
```

Рис. 2.10: Настройка интерфейсов коммутатора pisa-unipi-sw-1

Пропишем шлюз и ip-адрес на оконечном устройстве территории г. Пиза.

После проведем проверку и пропингуем устройства (рис. 2.11) (рис. 2.12) (рис. 2.13)

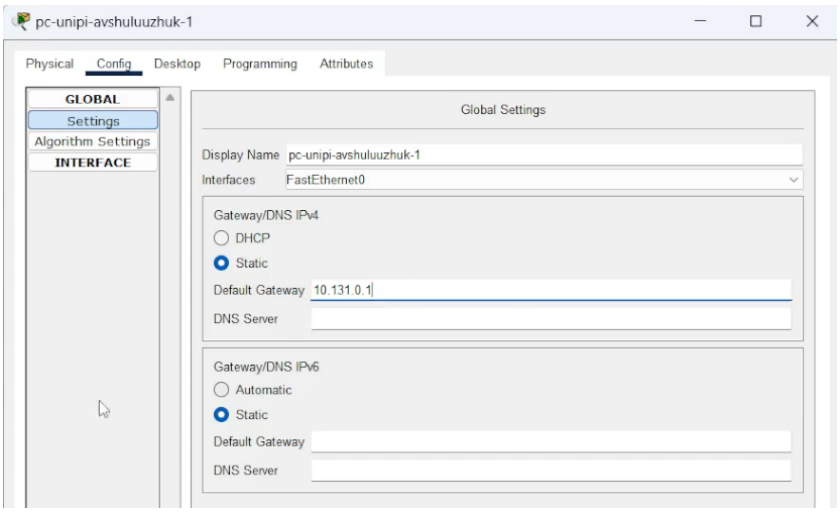


Рис. 2.11: Шлюз

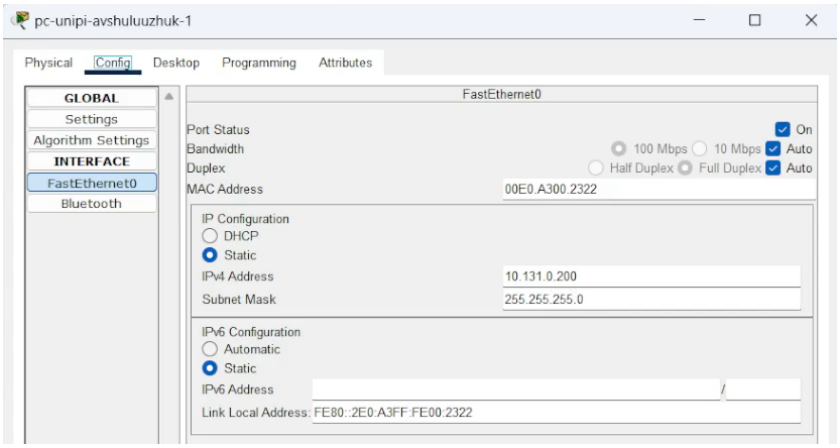


Рис. 2.12: IP-адресс

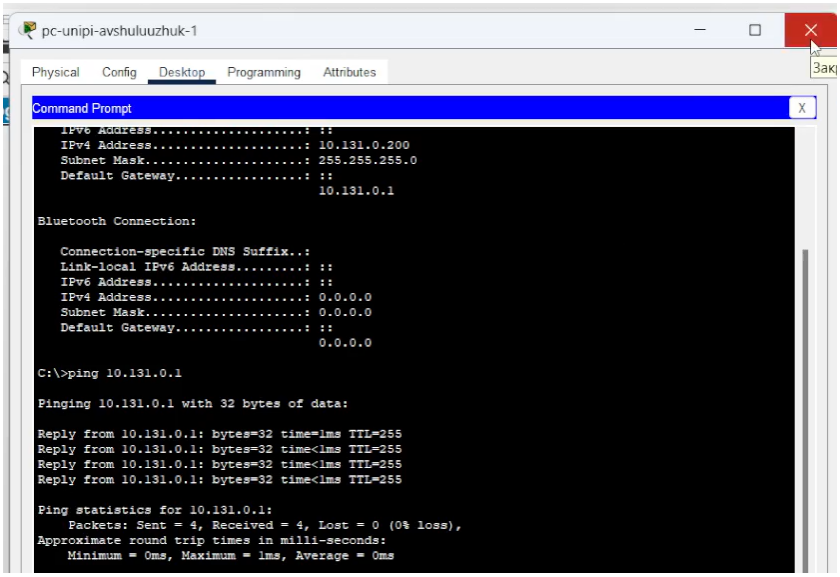


Рис. 2.13: Пингование устройств

Настроем VPN на основе протокола GRE (рис. 2.14) (рис. 2.15)

```
msk-donskaya-avshuluuzhuk-gw-1>en
Password:
msk-donskaya-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-avshuluuzhuk-gw-1(config)#interface Tunnel0

msk-donskaya-avshuluuzhuk-gw-1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

msk-donskaya-avshuluuzhuk-gw-1(config-if)#ip address 10.128.255.253 255.255.255.252
msk-donskaya-avshuluuzhuk-gw-1(config-if)#tunnel source f0/1.4
msk-donskaya-avshuluuzhuk-gw-1(config-if)#tunnel destination 192.0.2.20
msk-donskaya-avshuluuzhuk-gw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

msk-donskaya-avshuluuzhuk-gw-1(config-if)#exit
msk-donskaya-avshuluuzhuk-gw-1(config)#inteface loopback0
                                      ^
% Invalid input detected at '^' marker.

msk-donskaya-avshuluuzhuk-gw-1(config)#interface loopback0

msk-donskaya-avshuluuzhuk-gw-1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up

msk-donskaya-avshuluuzhuk-gw-1(config-if)#ip address 10.128.254.1 255.255.255.255
msk-donskaya-avshuluuzhuk-gw-1(config-if)#exit
msk-donskaya-avshuluuzhuk-gw-1(config)#ip route 10.128.254.5 255.255.255.255 10.128.255.254
msk-donskaya-avshuluuzhuk-gw-1(config)#^Z
msk-donskaya-avshuluuzhuk-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-donskaya-avshuluuzhuk-gw-1#
```

Рис. 2.14: Настройка маршрутизатора msk-donskaya-gw-1

```
pisa-unipi-avshuluuzhuk-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
pisa-unipi-avshuluuzhuk-gw-1(config)#interface Tunnel0

pisa-unipi-avshuluuzhuk-gw-1(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

pisa-unipi-avshuluuzhuk-gw-1(config-if)#ip address 10.128.255.254 255.255.255.252
pisa-unipi-avshuluuzhuk-gw-1(config-if)#tunnel source f0/1.4
%ERROR: Source interface does not exist.
pisa-unipi-avshuluuzhuk-gw-1(config-if)#tunnel source f0/1
pisa-unipi-avshuluuzhuk-gw-1(config-if)#tunnel destination 198.51.100.2
pisa-unipi-avshuluuzhuk-gw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

pisa-unipi-avshuluuzhuk-gw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#interface loopback0

pisa-unipi-avshuluuzhuk-gw-1(config-if)#
%LINK-5-CHANGED: Interface Loopback0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
\
                                        ^
% Invalid input detected at '^' marker.

pisa-unipi-avshuluuzhuk-gw-1(config-if)#ip address 10.128.254.5 255.255.255.255
pisa-unipi-avshuluuzhuk-gw-1(config-if)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#ip route 10.128.254.1 255.255.255.255 10.128.255.253
pisa-unipi-avshuluuzhuk-gw-1(config)#router ospf 1
pisa-unipi-avshuluuzhuk-gw-1(config-router)#router-id 10.128.254.5
pisa-unipi-avshuluuzhuk-gw-1(config-router)#network 10.0.0.0 0.255.255.255 area 0
pisa-unipi-avshuluuzhuk-gw-1(config-router)#exit
pisa-unipi-avshuluuzhuk-gw-1(config)#
01:23:19: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.1 on Tunnel0 from LOADING to FULL, Loading Done
```

Рис. 2.15: Настройка маршрутизатора pisa-unipi-gw-1

Проверим доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская» (рис. 2.16).

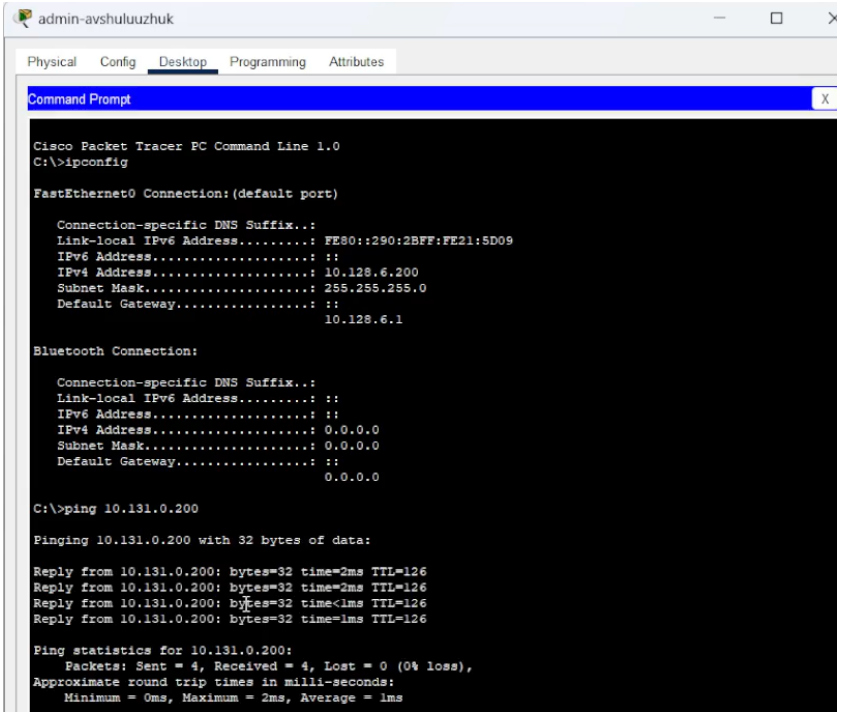


Рис. 2.16: Проверка доступности узлов г. Пиза

3 Выводы

В результате выполнения лабораторной работы были получечены навыки настройки VPN-туннеля через незащищённое Интернет-соединение.

4 Контрольные вопросы

1. **Что такое VPN?**

VPN (Virtual Private Network, виртуальная частная сеть) — это технология, которая создает защищённое и зашифрованное соединение между вашим устройством и удалённым сервером через интернет. Благодаря этому ваше интернет-соединение становится приватным и безопасным, а также позволяют скрыть ваш реальный IP-адрес и географическое положение.

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

   Защита личных данных и конфиденциальности при использовании публичных Wi-Fi сетей. Обход цензуры или блокировок сайтов и сервисов, ограниченных по регионам. Скрытие реального IP-адреса для анонимности в интернете. Получение доступа к контенту, доступному только в определённых странах. Обеспечение безопасности при удалённой работе и подключении к корпоративной сети. Защита от слежки со стороны провайдеров и государственных органов.

3. **Как с помощью VPN обойти NAT?**

NAT (Network Address Translation) — это технология, которая позволяет нескольким устройствам в локальной сети использовать один публичный IP-адрес для выхода в интернет. В большинстве случаев NAT не мешает использованию VPN, однако иногда могут возникать сложности с пробросом портов или соединениями, требующими входящих подключений.

Обойти ограничения NAT с помощью VPN можно следующим образом:

Использовать VPN-сервисы, поддерживающие протоколы, позволяющие проброс портов или раб
Настроить VPN на уровне маршрутизатора, чтобы все устройства сети автоматически исполь
Использовать протоколы VPN, которые хорошо работают с NAT, например, OpenVPN с настрой
оболочки.
В случае необходимости – настроить порт-форвардинг или использовать VPN-
сервисы, предоставляющие статические IP-адреса или специальные функции обхода NAT.