

# **Отчёт по лабораторной работе №16**

**Администрирование локальных сетей**

Бансимба Клодели Дъегра, НПИбд-02-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>3</b>	<b>Выводы</b>	<b>12</b>
<b>4</b>	<b>Ответы на контрольные вопросы:</b>	<b>13</b>

## Список иллюстраций

2.1	Открытие проекта lab_PT-16.pkt. . . . .	6
2.2	Замена модулей на Repeater-PT. . . . .	6
2.3	Подключение оборудования. В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза. Переместим туда соответствующее оборудование . . . . .	7
2.4	Создание города Пиза в физической рабочей области. . . . .	7
2.5	Перемещение оборудования. Теперь сделаем первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза . . . . .	7
2.6	Первоначальная настройка маршрутизатора pisa-unipi-claude-gw-1. . . . .	8
2.7	Первоначальная настройка коммутатора pisa-unipi-claude-sw-1. . . . .	8
2.8	Настройка интерфейсов маршрутизатора pisa-unipi-claude-gw-1. . . . .	9
2.9	Настройка интерфейсов маршрутизатора pisa-unipi-claude-gw-1. . . . .	9
2.10	Присвоение адресов оконечному устройству. . . . .	10
2.11	Пинг адреса 10.131.0.1. . . . .	10
2.12	Настройка маршрутизатора msk-donskaya-claudehorin-gw-1. . . . .	11

## **Список таблиц**

# 1 Цель работы

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

## 2 Выполнение лабораторной работы

Откроем проект с названием lab\_PT-15.pkt и сохраним под названием lab\_PT-16.pkt. После чего откроем его для дальнейшего редактирования (рис. fig. 2.1).

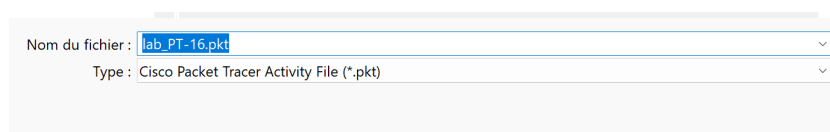


Рис. 2.1: Открытие проекта lab\_PT-16.pkt.

Разместим в рабочей области проекта в соответствии с модельными предположениями оборудование для сети Университета г. Пиза

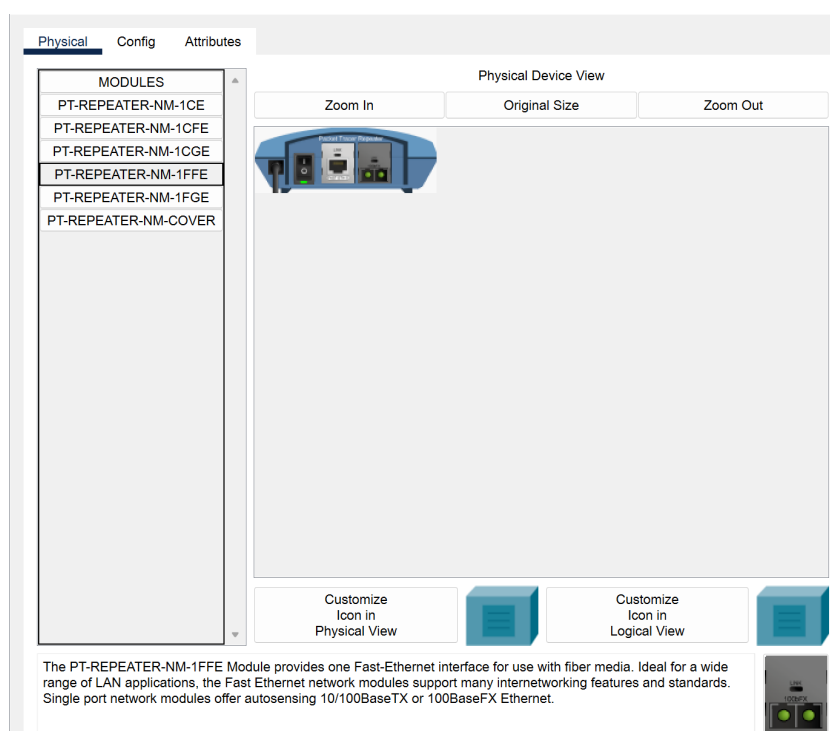


Рис. 2.2: Замена модулей на Repeater-PT.

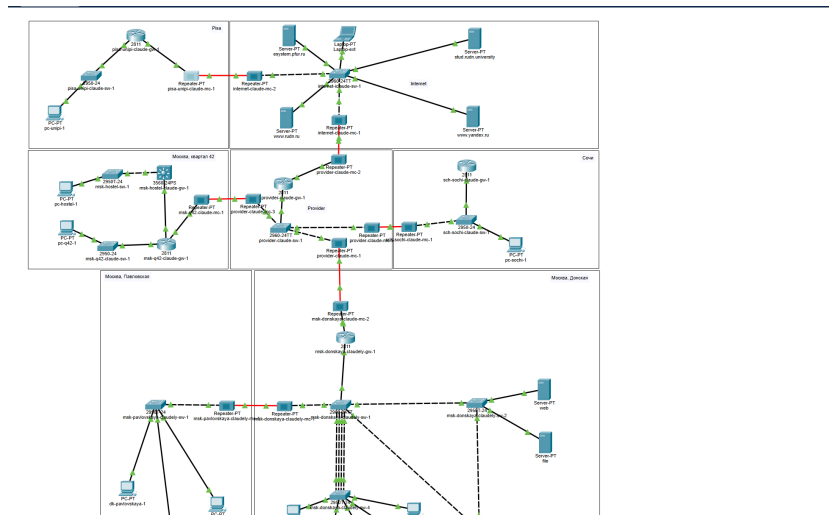


Рис. 2.3: Подключение оборудования. В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза. Переместим туда соответствующее оборудование

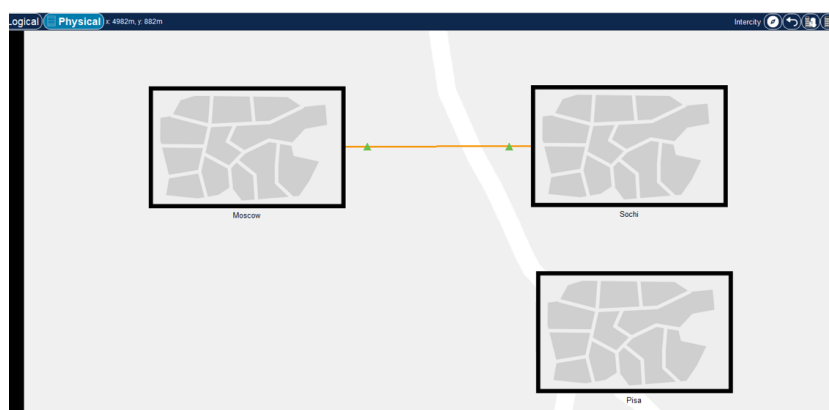


Рис. 2.4: Создание города Пиза в физической рабочей области.

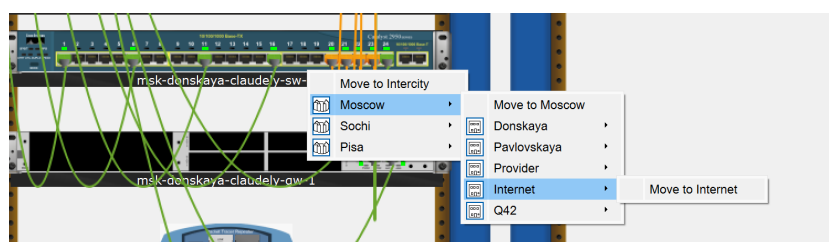
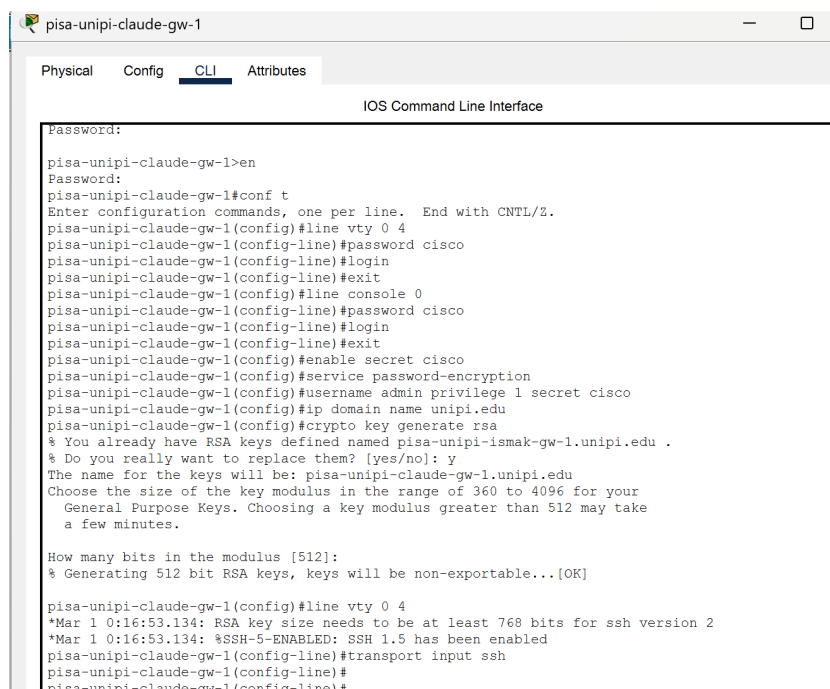


Рис. 2.5: Перемещение оборудования. Теперь сделаем первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза



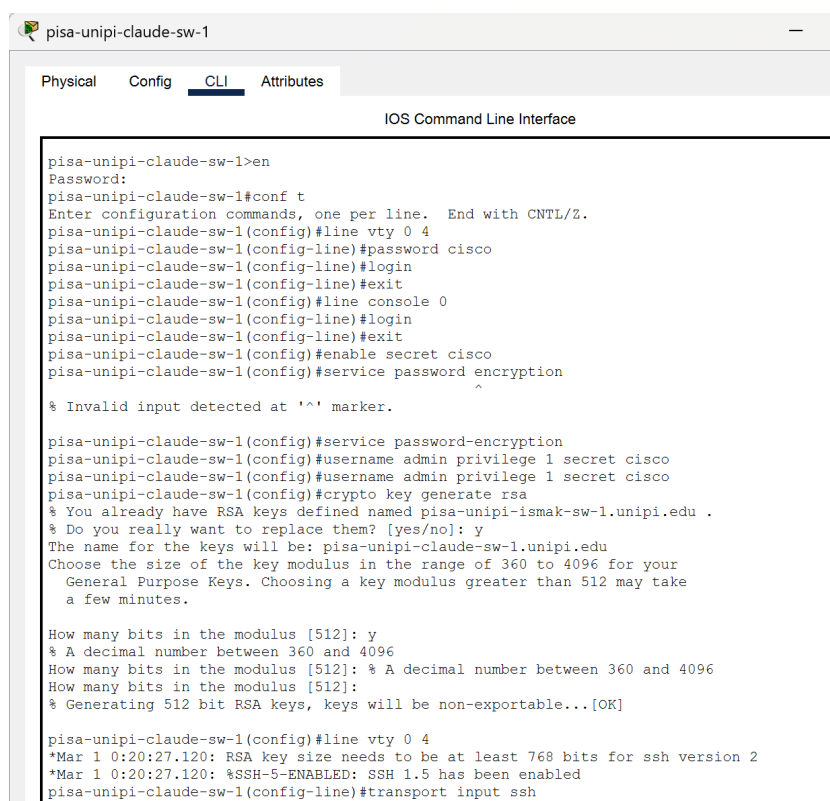
```
pisa-unipi-claude-gw-1
Physical Config CLI Attributes
IOS Command Line Interface

Password:
pisa-unipi-claude-gw-1>en
Password:
pisa-unipi-claude-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
pisa-unipi-claude-gw-1(config)#line vty 0 4
pisa-unipi-claude-gw-1(config-line)#password cisco
pisa-unipi-claude-gw-1(config-line)#login
pisa-unipi-claude-gw-1(config-line)#exit
pisa-unipi-claude-gw-1(config)#line console 0
pisa-unipi-claude-gw-1(config-line)#password cisco
pisa-unipi-claude-gw-1(config-line)#login
pisa-unipi-claude-gw-1(config-line)#exit
pisa-unipi-claude-gw-1(config)#enable secret cisco
pisa-unipi-claude-gw-1(config)#service password-encryption
pisa-unipi-claude-gw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-claude-gw-1(config)#ip domain name unipi.edu
pisa-unipi-claude-gw-1(config)#crypto key generate rsa
% You already have RSA keys defined named pisa-unipi-ismak-gw-1.unipi.edu .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: pisa-unipi-claude-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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-claude-gw-1(config)#line vty 0 4
*Mar 1 0:16:53.134: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:16:53.134: %SSH-5-ENABLED: SSH 1.5 has been enabled
pisa-unipi-claude-gw-1(config-line)#transport input ssh
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
```

Рис. 2.6: Первоначальная настройка маршрутизатора pisa-unipi-claude-gw-1.



```
pisa-unipi-claude-sw-1
Physical Config CLI Attributes
IOS Command Line Interface

pisa-unipi-claude-sw-1>en
Password:
pisa-unipi-claude-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
pisa-unipi-claude-sw-1(config)#line vty 0 4
pisa-unipi-claude-sw-1(config-line)#password cisco
pisa-unipi-claude-sw-1(config-line)#login
pisa-unipi-claude-sw-1(config-line)#exit
pisa-unipi-claude-sw-1(config)#line console 0
pisa-unipi-claude-sw-1(config-line)#login
pisa-unipi-claude-sw-1(config-line)#exit
pisa-unipi-claude-sw-1(config)#enable secret cisco
pisa-unipi-claude-sw-1(config)#service password encryption
^
% Invalid input detected at '^' marker.

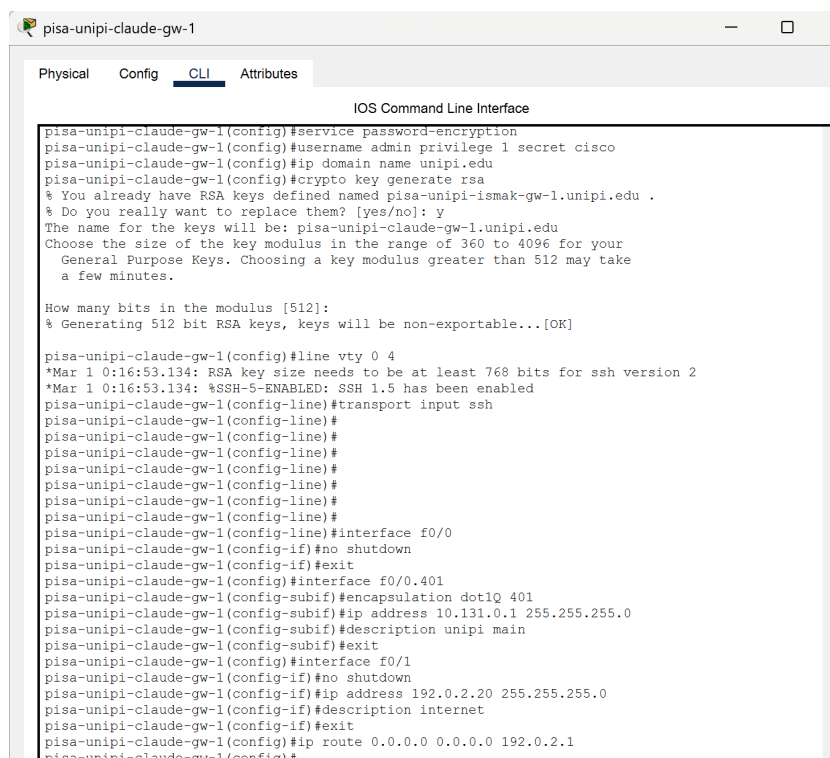
pisa-unipi-claude-sw-1(config)#service password-encryption
pisa-unipi-claude-sw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-claude-sw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-claude-sw-1(config)#crypto key generate rsa
% You already have RSA keys defined named pisa-unipi-ismak-sw-1.unipi.edu .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: pisa-unipi-claude-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]: y
% A decimal number between 360 and 4096
How many bits in the modulus [512]: % A decimal number between 360 and 4096
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-claude-sw-1(config)#line vty 0 4
*Mar 1 0:20:27.120: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:20:27.120: %SSH-5-ENABLED: SSH 1.5 has been enabled
pisa-unipi-claude-sw-1(config-line)#transport input ssh
```

Рис. 2.7: Первоначальная настройка коммутатора pisa-unipi-claude-sw-1.





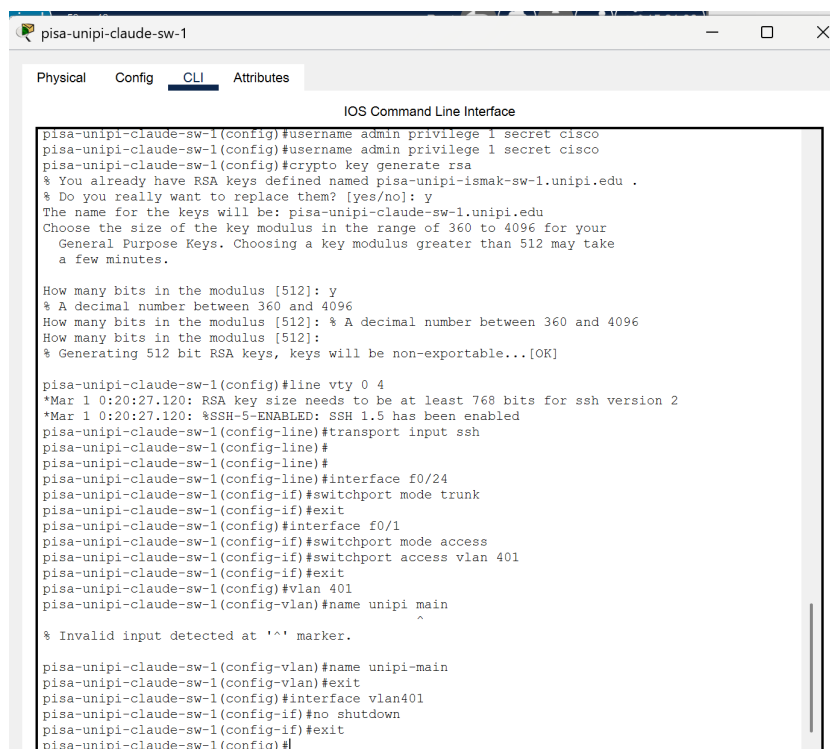
```
pisa-unipi-claude-gw-1
Physical Config CLI Attributes
IOS Command Line Interface

pisa-unipi-claude-gw-1(config)#service password-encryption
pisa-unipi-claude-gw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-claude-gw-1(config)#ip domain name unipi.edu
pisa-unipi-claude-gw-1(config)#crypto key generate rsa
% You already have RSA keys defined named pisa-unipi-ismak-gw-1.unipi.edu .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: pisa-unipi-claude-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]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-claude-gw-1(config)#line vty 0 4
*Mar 1 0:16:53.134: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:16:53.134: %SSH-5-ENABLED: SSH 1.5 has been enabled
pisa-unipi-claude-gw-1(config-line)#transport input ssh
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#
pisa-unipi-claude-gw-1(config-line)#interface f0/0
pisa-unipi-claude-gw-1(config-if)#no shutdown
pisa-unipi-claude-gw-1(config-if)#exit
pisa-unipi-claude-gw-1(config)#interface f0/0.401
pisa-unipi-claude-gw-1(config-subif)#encapsulation dot1Q 401
pisa-unipi-claude-gw-1(config-subif)#ip address 10.131.0.1 255.255.255.0
pisa-unipi-claude-gw-1(config-subif)#description unipi main
pisa-unipi-claude-gw-1(config-subif)#exit
pisa-unipi-claude-gw-1(config)#interface f0/1
pisa-unipi-claude-gw-1(config-if)#no shutdown
pisa-unipi-claude-gw-1(config-if)#ip address 192.0.2.20 255.255.255.0
pisa-unipi-claude-gw-1(config-if)#description internet
pisa-unipi-claude-gw-1(config-if)#exit
pisa-unipi-claude-gw-1(config)#ip route 0.0.0.0 0.0.0.0 192.0.2.1
pisa-unipi-claude-gw-1(config)#
```

Рис. 2.8: Настройка интерфейсов маршрутизатора pisa-unipi-claude-gw-1.



```
pisa-unipi-claude-sw-1
Physical Config CLI Attributes
IOS Command Line Interface

pisa-unipi-claude-sw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-claude-sw-1(config)#username admin privilege 1 secret cisco
pisa-unipi-claude-sw-1(config)#crypto key generate rsa
% You already have RSA keys defined named pisa-unipi-ismak-sw-1.unipi.edu .
% Do you really want to replace them? [yes/no]: y
The name for the keys will be: pisa-unipi-claude-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]: y
% A decimal number between 360 and 4096
How many bits in the modulus [512]: % A decimal number between 360 and 4096
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

pisa-unipi-claude-sw-1(config)#line vty 0 4
*Mar 1 0:20:27.120: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:20:27.120: %SSH-5-ENABLED: SSH 1.5 has been enabled
pisa-unipi-claude-sw-1(config-line)#transport input ssh
pisa-unipi-claude-sw-1(config-line)#
pisa-unipi-claude-sw-1(config-line)#
pisa-unipi-claude-sw-1(config-line)#interface f0/24
pisa-unipi-claude-sw-1(config-if)#switchport mode trunk
pisa-unipi-claude-sw-1(config-if)#exit
pisa-unipi-claude-sw-1(config)#interface f0/1
pisa-unipi-claude-sw-1(config-if)#switchport mode access
pisa-unipi-claude-sw-1(config-if)#switchport access vlan 401
pisa-unipi-claude-sw-1(config-if)#exit
pisa-unipi-claude-sw-1(config)#vlan 401
pisa-unipi-claude-sw-1(config-vlan)#name unipi main
pisa-unipi-claude-sw-1(config-vlan)#
% Invalid input detected at '^' marker.

pisa-unipi-claude-sw-1(config-vlan)#name unipi-main
pisa-unipi-claude-sw-1(config-vlan)#exit
pisa-unipi-claude-sw-1(config)#interface vlan401
pisa-unipi-claude-sw-1(config-if)#no shutdown
pisa-unipi-claude-sw-1(config-if)#exit
pisa-unipi-claude-sw-1(config)#
```

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

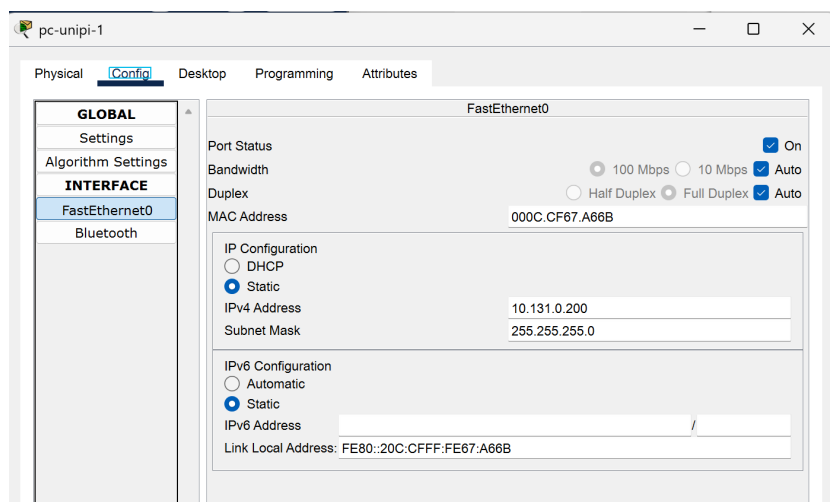


Рис. 2.10: Присвоение адресов оконечному устройству.

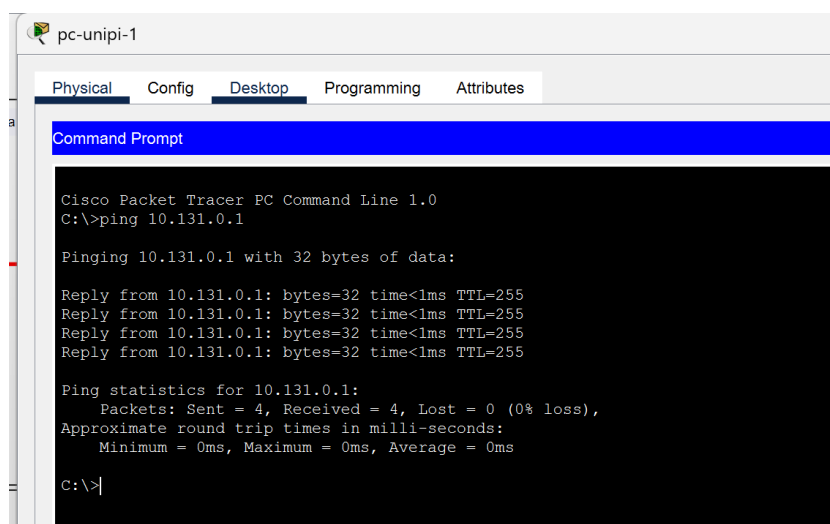
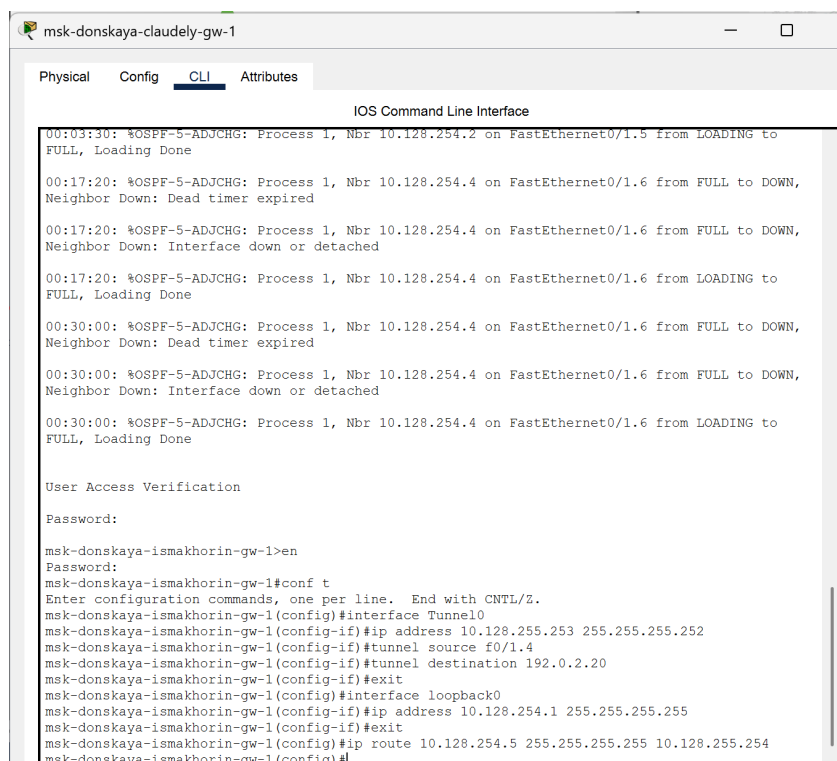


Рис. 2.11: Пинг адреса 10.131.0.1.

Далее настроим VPN на основе протокола GRE [25]



```
msk-donskaya-claudely-gw-1
Physical Config CLI Attributes
IOS Command Line Interface
00:03:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.2 on FastEthernet0/1.5 from LOADING to FULL, Loading Done
00:17:20: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.4 on FastEthernet0/1.6 from FULL to DOWN, Neighbor Down: Dead timer expired
00:17:20: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.4 on FastEthernet0/1.6 from FULL to DOWN, Neighbor Down: Interface down or detached
00:17:20: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.4 on FastEthernet0/1.6 from LOADING to FULL, Loading Done
00:30:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.4 on FastEthernet0/1.6 from FULL to DOWN, Neighbor Down: Dead timer expired
00:30:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.4 on FastEthernet0/1.6 from FULL to DOWN, Neighbor Down: Interface down or detached
00:30:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.128.254.4 on FastEthernet0/1.6 from LOADING to FULL, Loading Done
User Access Verification
Password:
msk-donskaya-ismakhorin-gw-1>en
Password:
msk-donskaya-ismakhorin-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-ismakhorin-gw-1(config)#interface Tunnel0
msk-donskaya-ismakhorin-gw-1(config-if)#ip address 10.128.255.253 255.255.255.252
msk-donskaya-ismakhorin-gw-1(config-if)#tunnel source f0/1.4
msk-donskaya-ismakhorin-gw-1(config-if)#tunnel destination 192.0.2.20
msk-donskaya-ismakhorin-gw-1(config-if)#exit
msk-donskaya-ismakhorin-gw-1(config)#interface loopback0
msk-donskaya-ismakhorin-gw-1(config-if)#ip address 10.128.254.1 255.255.255.255
msk-donskaya-ismakhorin-gw-1(config-if)#exit
msk-donskaya-ismakhorin-gw-1(config)#ip route 10.128.254.5 255.255.255.255 10.128.255.254
msk-donskaya-ismakhorin-gw-1(config)#
```

Рис. 2.12: Настройка маршрутизатора msk-donskaya-claudehorin-gw-1.

![Настройка маршрутизатора pisa-unipi-claude-gw-1.] (image/1.png){#fig:001 width=70%}%}

## **3 Выводы**

В ходе выполнения лабораторной работы мы получили навыки настройки VPN-туннеля через незащищённое Интернет-соединение.

## **4 Ответы на контрольные вопросы:**

1. Что такое VPN? - Зашифрованное соединение, устанавливаемое через Интернет между устройством и сетью.
2. В каких случаях следует использовать VPN? - Для дополнительного шифрования в сетях, безопасному подключению к локальным сетям извне.
3. Как с помощью VPN обойти NAT? - Поднять VPN-туннель/подключить OpenVPN.