Настройка VPN

Лабораторная работа № 16

Шулуужук Айраана НПИбд-02-22

Содержание

# 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. 1) (рис. 2) (рис. 3)

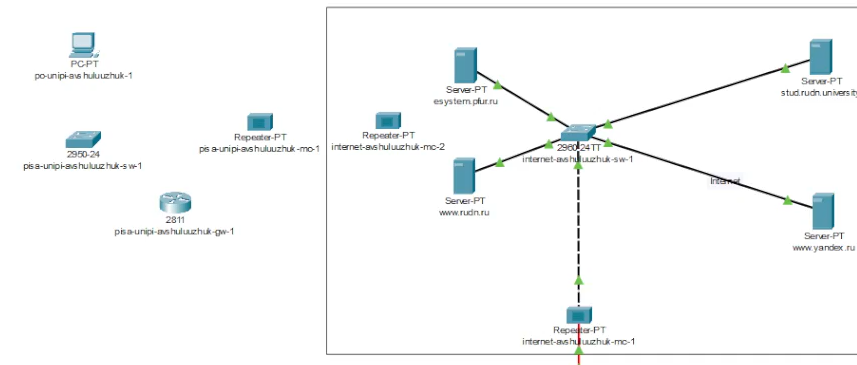


Рис. 1: Раземещение необходимого оборудования в сеть



Рис. 2: Настройка портов на медиаконвертерах

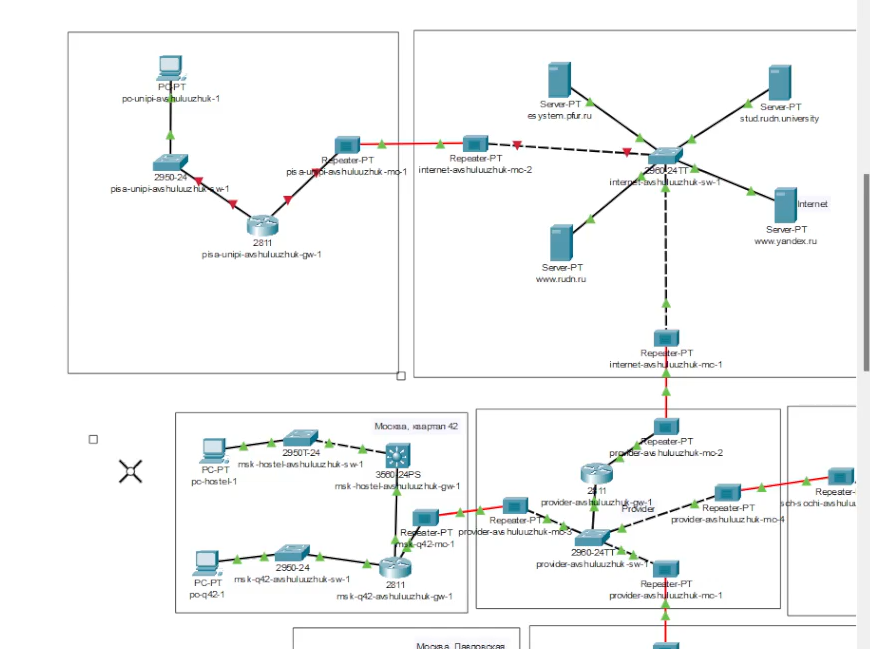


Рис. 3: Проведение соединеия оборудования

В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза. Переместим туда соответствующее оборудование (рис. 4) (рис. 5) (рис. 6)

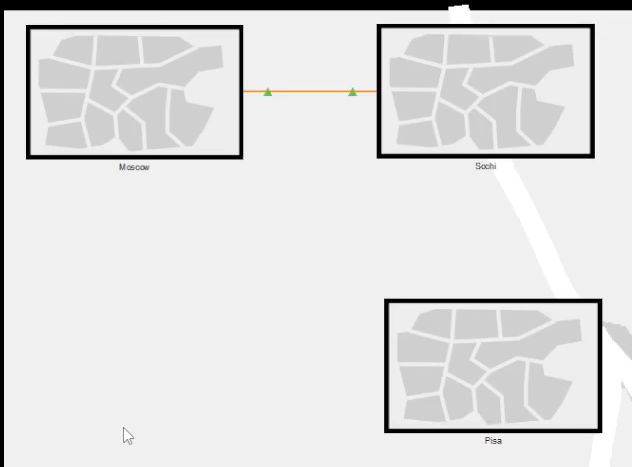


Рис. 4: Создание города Пиза

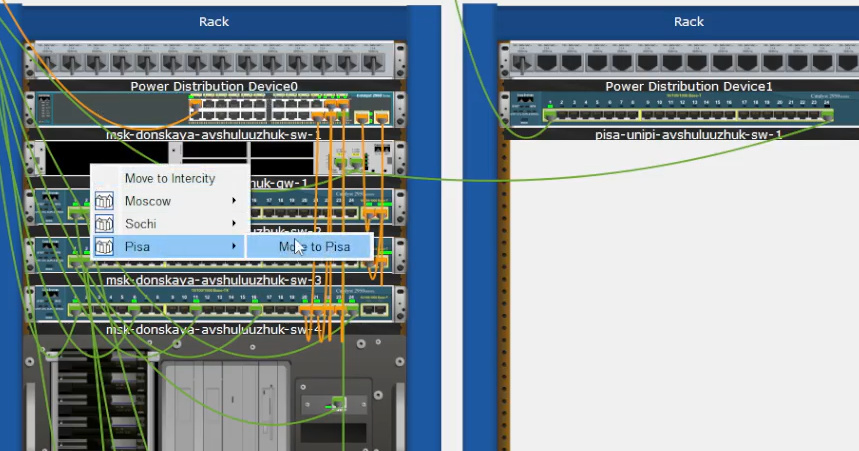


Рис. 5: Перемещение оборудования на соответствующие территории

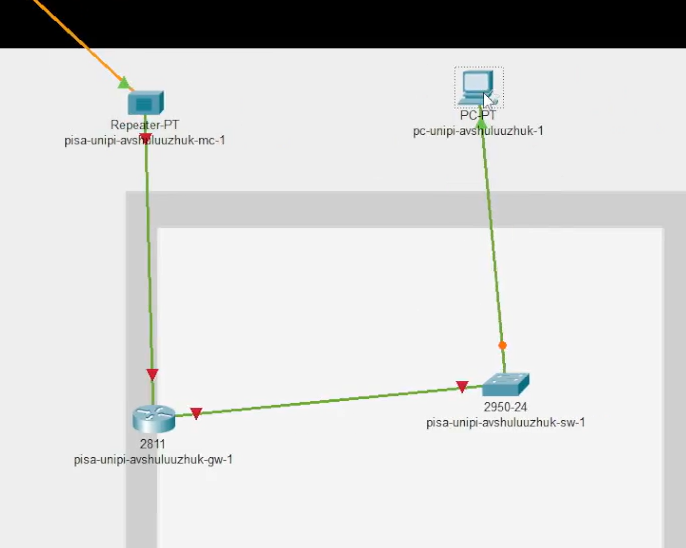


Рис. 6: Оборудование на территории г. Пиза

Сделаем первоначальную настройку и настройку интерфейсов оборудования сети Университета г. Пиза (рис. 7) (рис. 8 (рис. 9) (рис. 10)

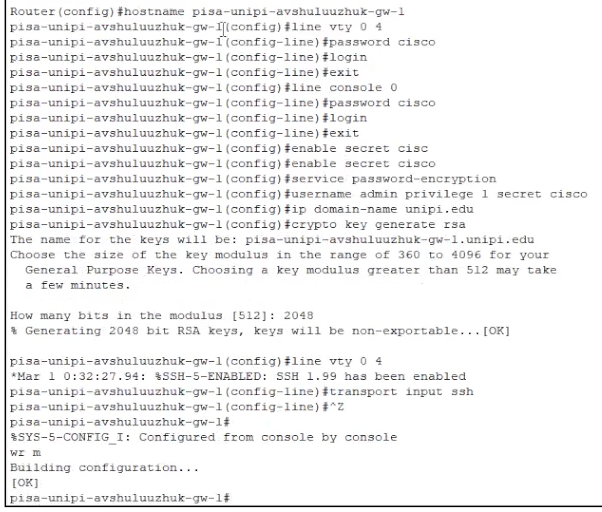


Рис. 7: Первоначальная настройка маршрутизатора pisa-unipi-gw-1

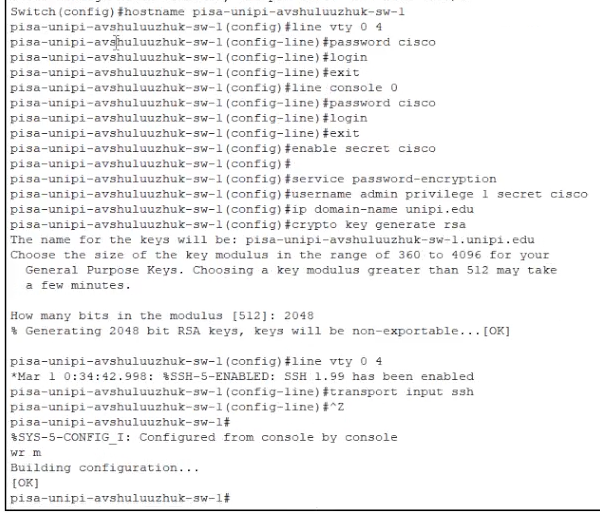


Рис. 8: Первоначальная настройка коммутатора pisa-unipi-sw-1

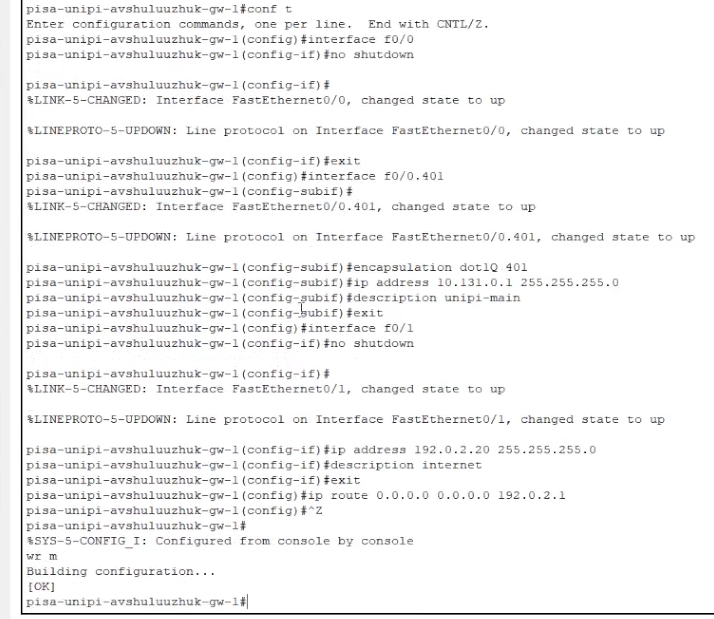


Рис. 9: Настройка интерфейсов маршрутизатора pisa-unipi-gw-1

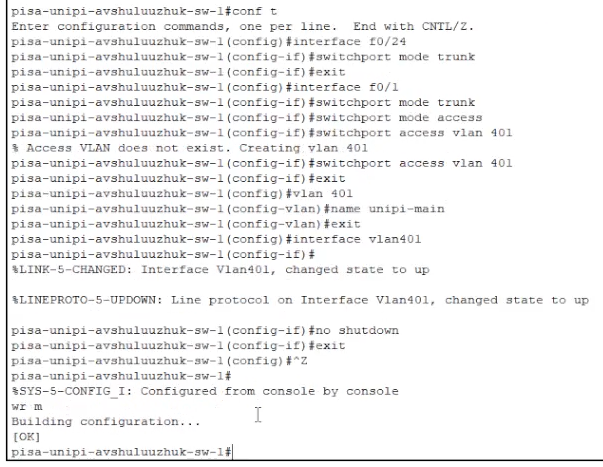


Рис. 10: Настройка интерфейсов коммутатора pisa-unipi-sw-1

Пропишем шлюз и ip-адрес на оконечном устройстве территории г. Пиза. После проведем проверку и пропингуем устройства (рис. 11) (рис. 12) (рис. 13)

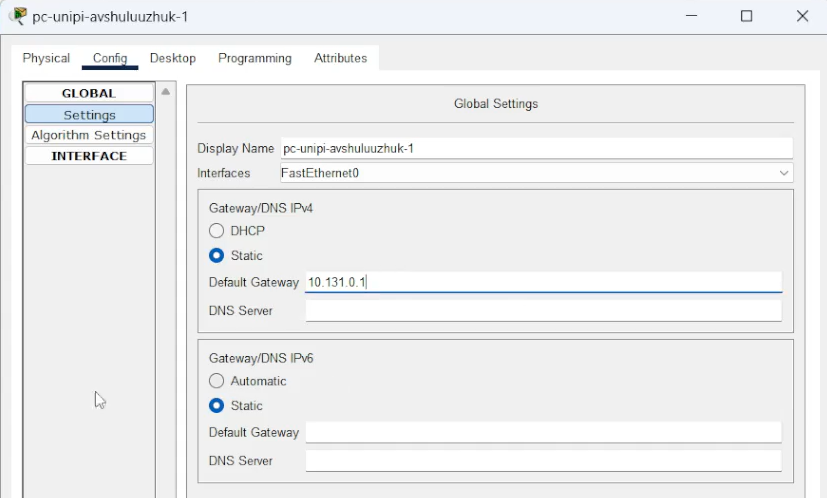


Рис. 11: Шлюз

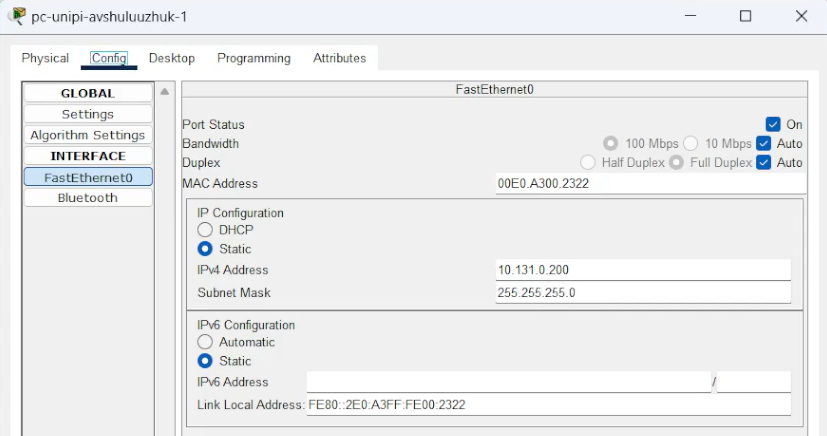


Рис. 12: IP-адресс

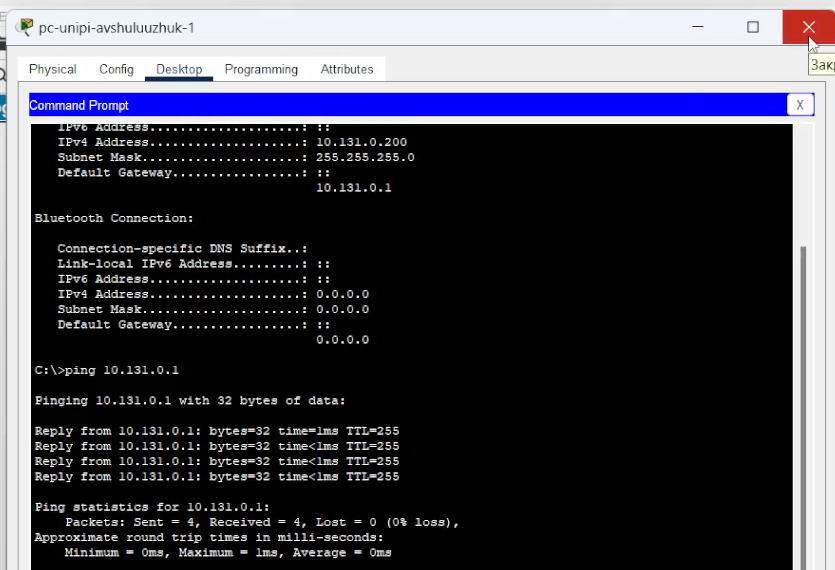


Рис. 13: Пингование устройств

Настроем VPN на основе протокола GRE (рис. 14) (рис. 15)

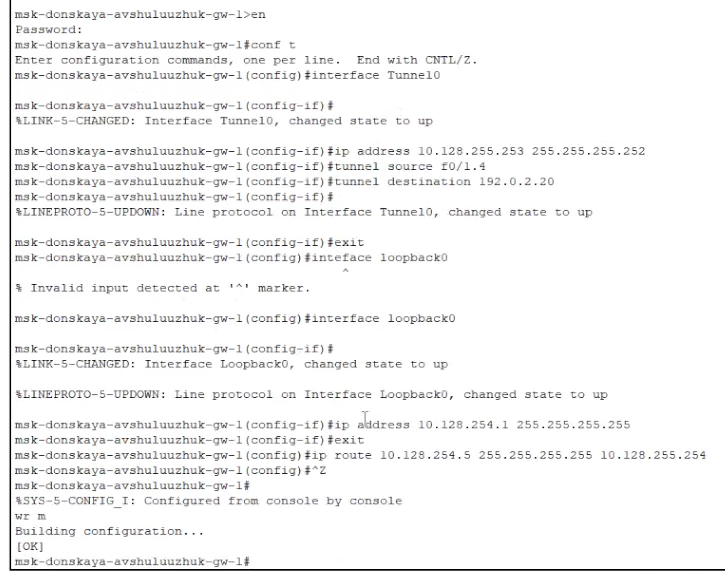


Рис. 14: Настройка маршрутизатора msk-donskaya-gw-1

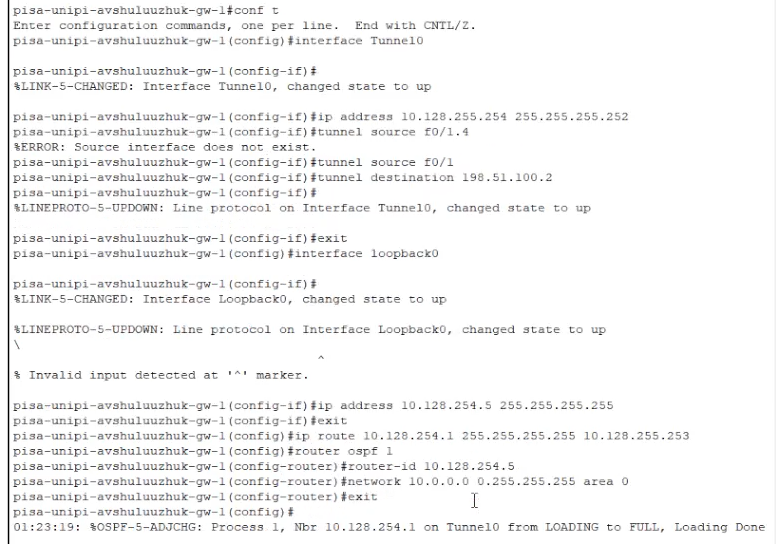


Рис. 15: Настройка маршрутизатора pisa-unipi-gw-1

Проверим доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская» (рис. 16).

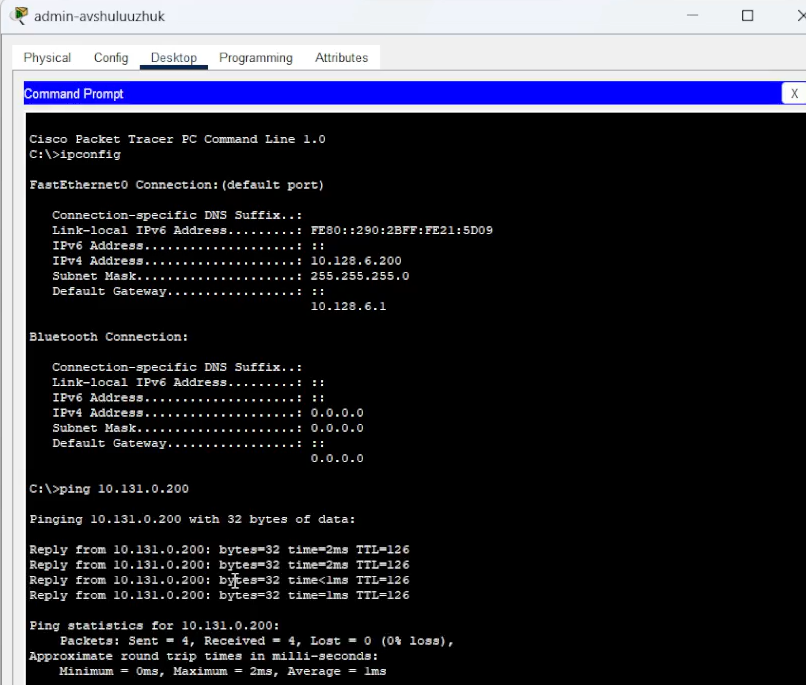


Рис. 16: Проверка доступности узлов г. Пиза

# 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.

1. 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.

1. 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 работу с режимом "VPN Passthrough".  
Настроить VPN на уровне маршрутизатора, чтобы все устройства сети автоматически использовали VPN, обеспечивая более стабильное соединение.  
Использовать протоколы VPN, которые хорошо работают с NAT, например, OpenVPN с настройками для обхода NAT или протоколы, использующие UDP-оболочки.  
В случае необходимости — настроить порт-форвардинг или использовать VPN-сервисы, предоставляющие статические IP-адреса или специальные функции обхода NAT.