Отчёт по лабораторной работе №16

Администрирование локальных сетей

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

Получение навыков настройки VPN-туннеля через незащищённое Интернетсоединение [**netadmin?**].

# 2 Задание

Настроить VPN-туннель между сетью Университета г. Пиза (Италия) и сетью «Донская» в г. Москва.

# 3 Выполнение лабораторной работы

Сеть Университета г. Пиза (Италия) содержит маршрутизатор Cisco 2811 pisa-inipi-gw-1, коммутатор Cisco 2950 pisa-unipi-sw-1 и конечное устройство PC pc-unipi-1. Разместим оборудование в рабочей области проекта. Изменим модули медиаконвертера (рис. 1).

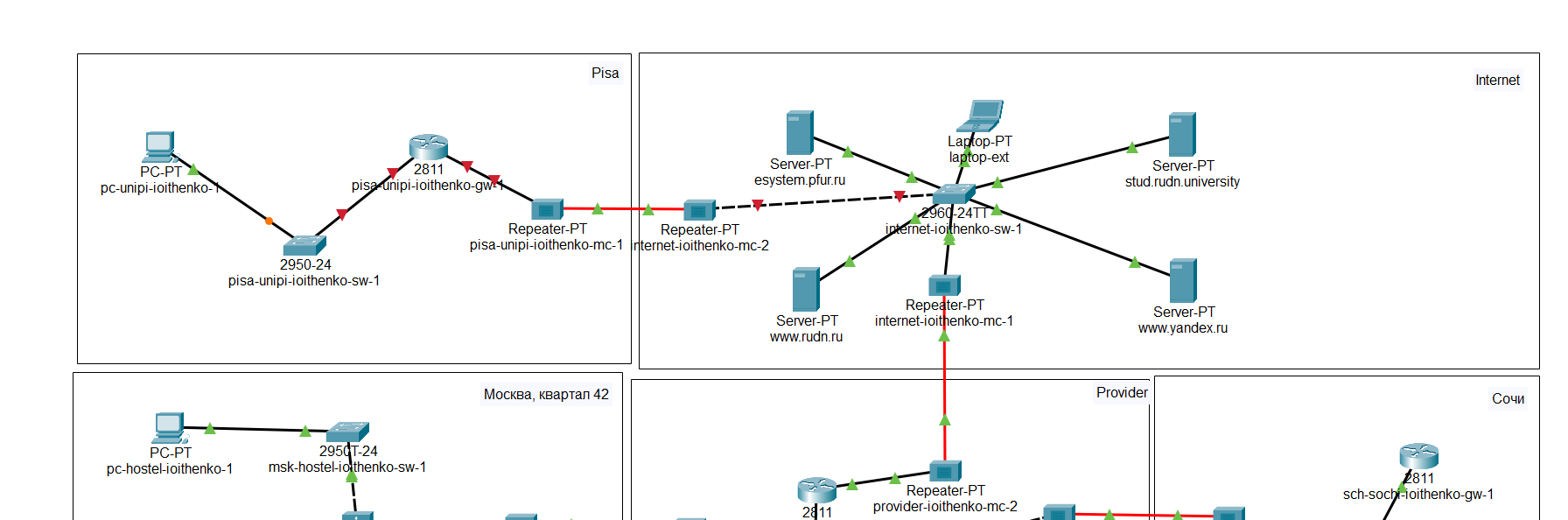


Рис. 1: Размещение оборудования

В физической рабочей области проекта создадим город Пиза, здание Университета г. Пиза. Переместим туда соответствующее оборудование (рис. 2).

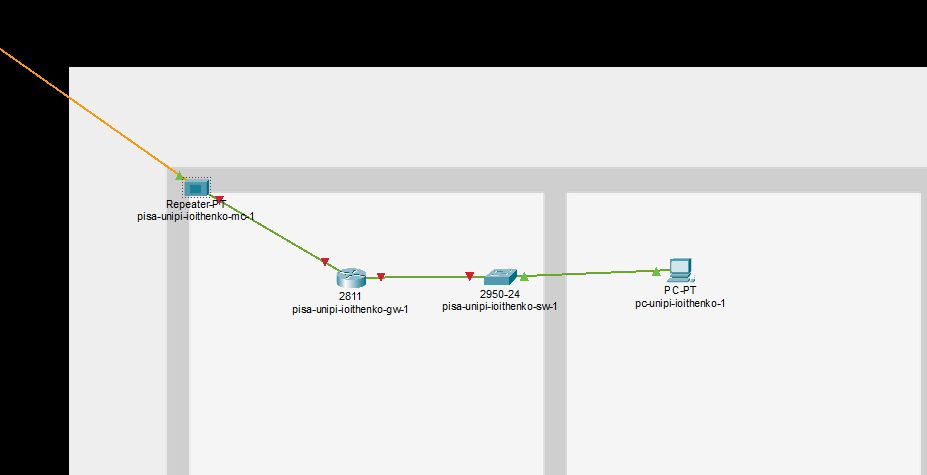


Рис. 2: Физическая область

Сделаем первоначальную настройку маршрутизатора Университета г. Пиза (рис. 3).

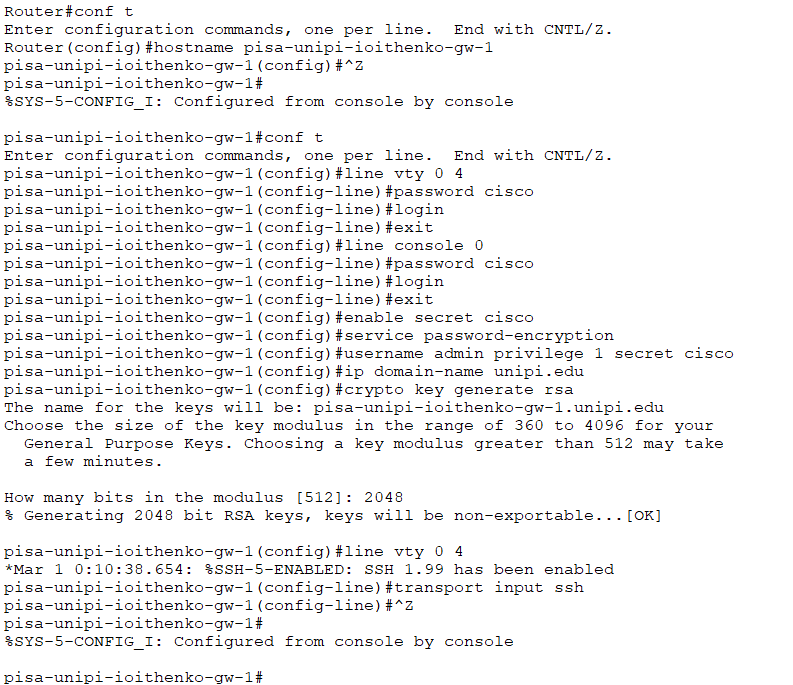


Рис. 3: Первоначальная настройка

Сделаем первоначальную настройку коммутатора Университета г. Пиза (рис. 4).

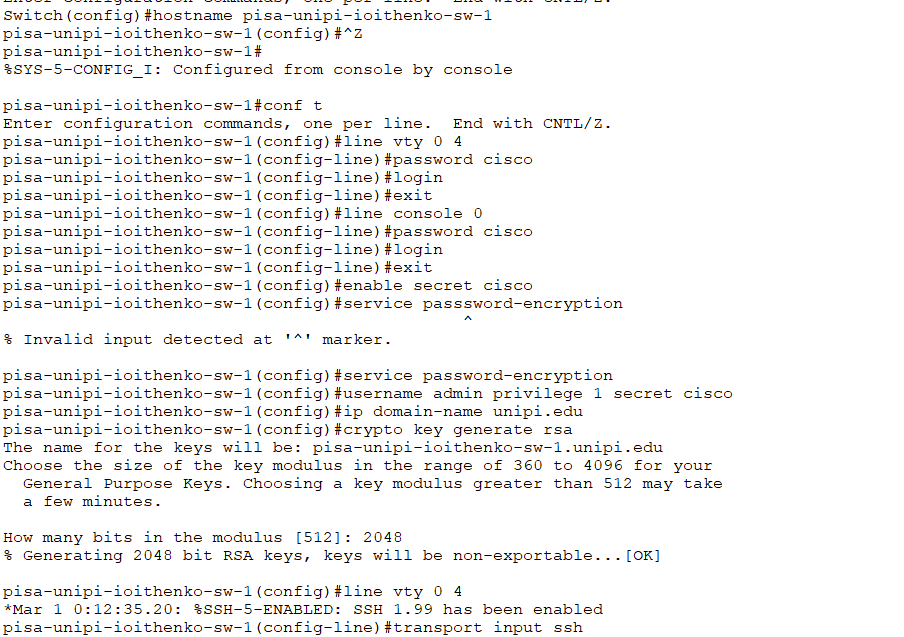


Рис. 4: Первоначальная настройка

Сделаем настройку интерфейсов коммутатора Университета г. Пиза (рис. 5).

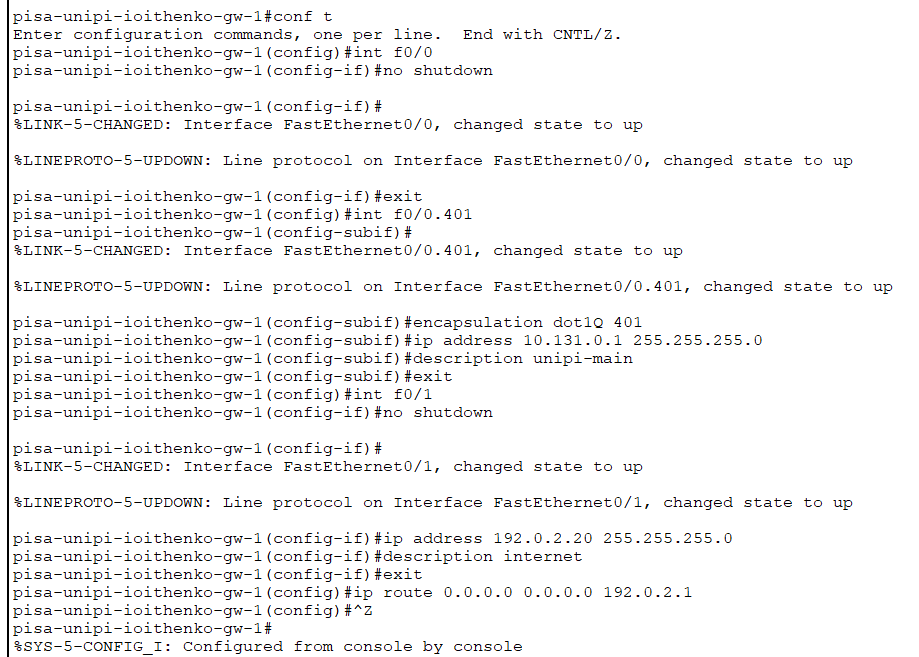


Рис. 5: Настройка интерфейсов

Сделаем настройку интерфейсов коммутатора Университета г. Пиза (рис. 6).

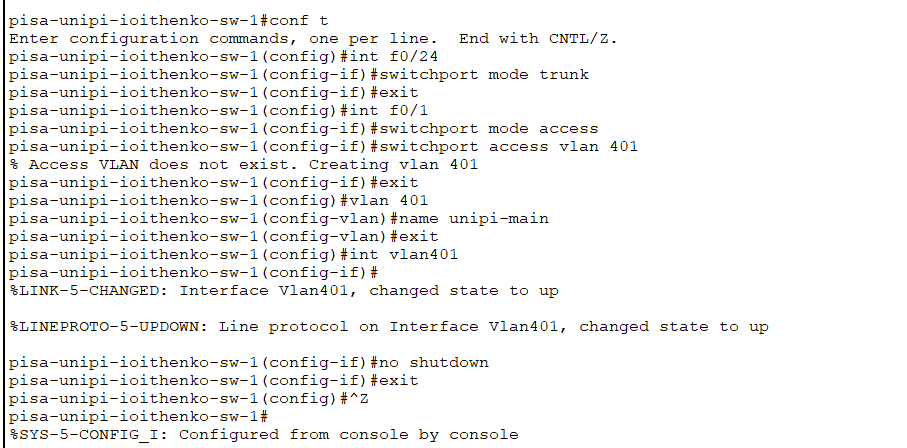


Рис. 6: Настройка интерфейсов

Зададим IP-адрес оконечному устройству и проверим работоспособность (рис. 7).

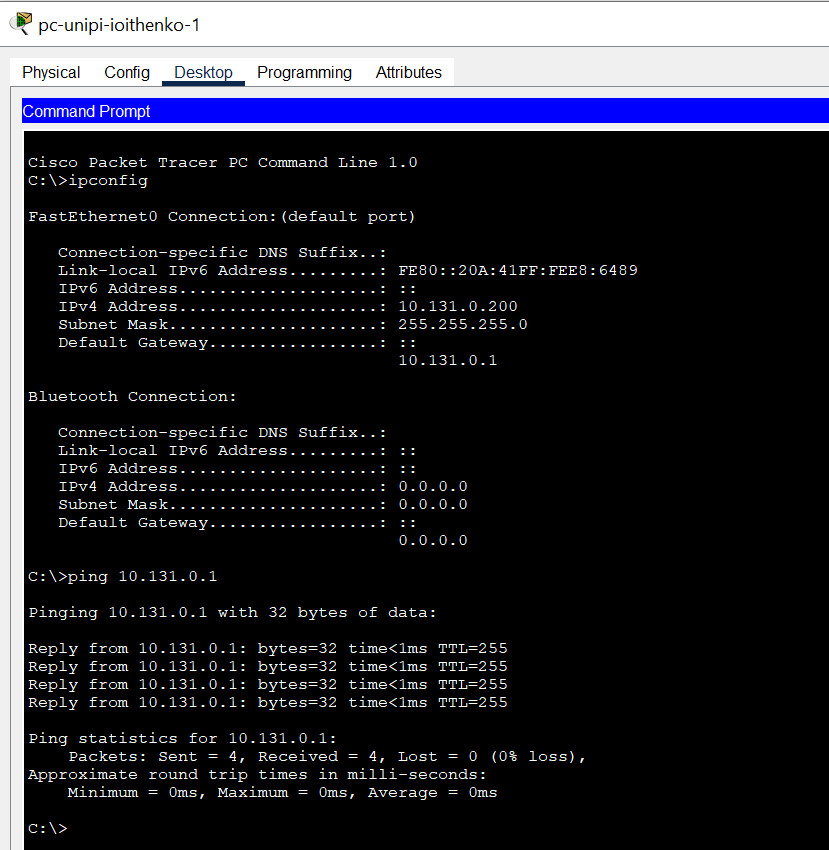


Рис. 7: Проверка

Настроим VPN на основе протокола GRE (рис. 8) и (рис. 9).

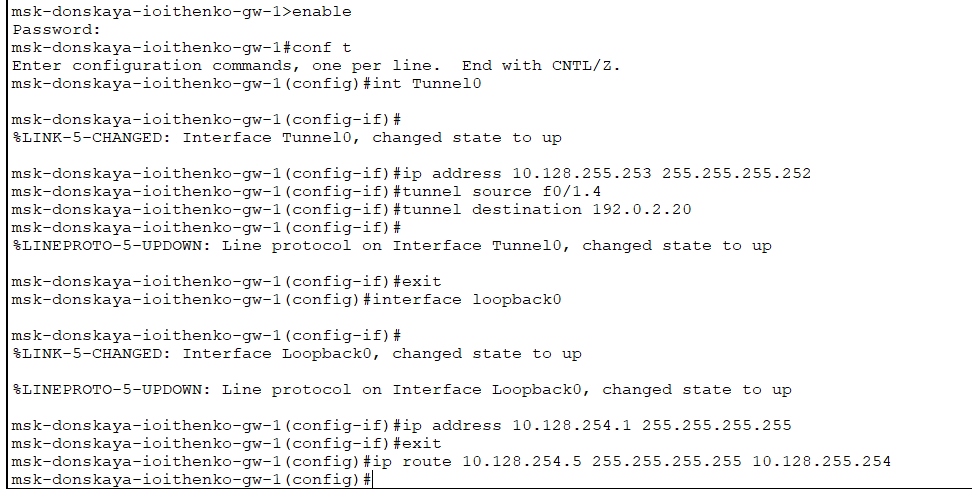


Рис. 8: Настройка VPN

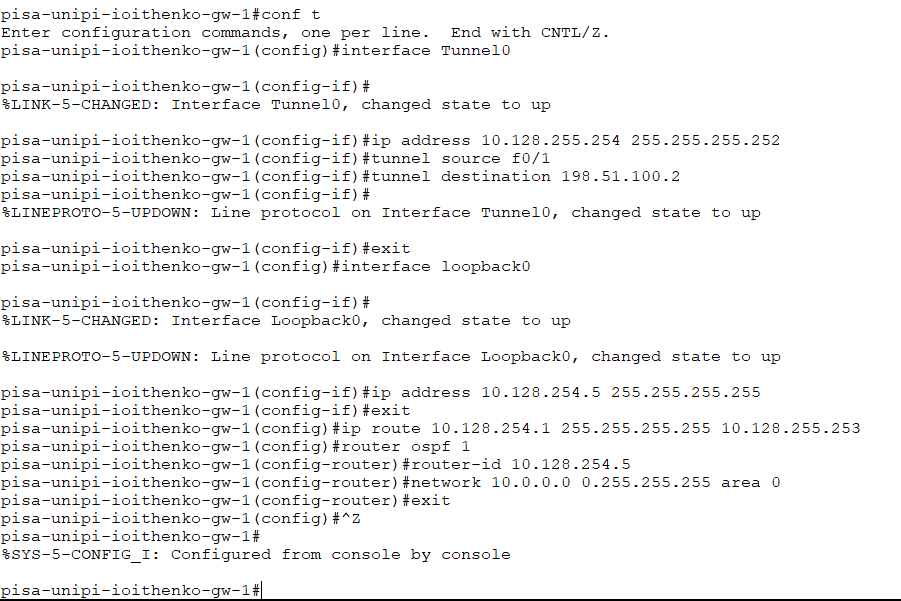


Рис. 9: Настройка VPN

Проверим доступность узлов сети Университета г. Пиза с ноутбука администратора сети «Донская». Доступно (рис. 10).

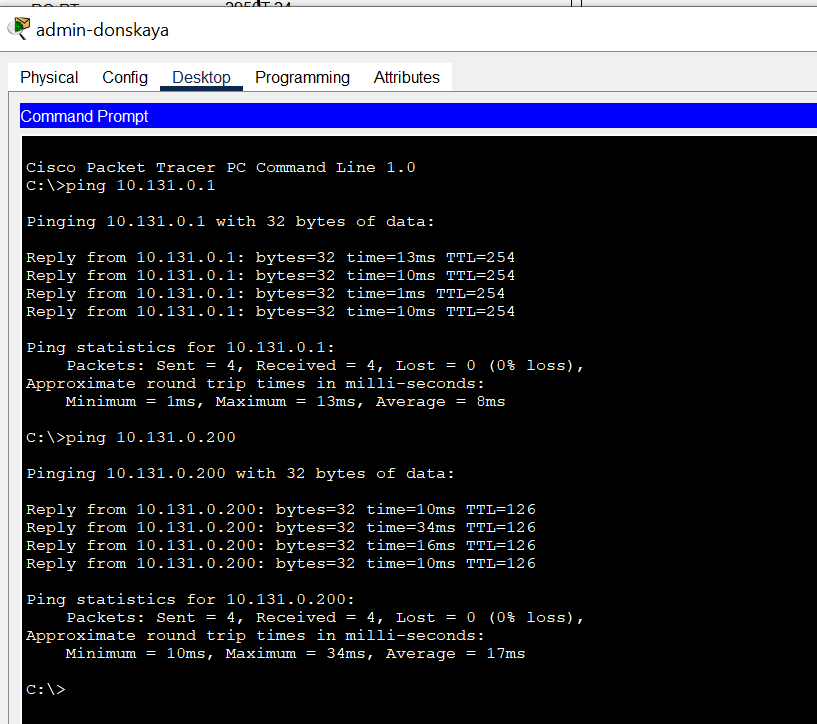


Рис. 10: Настройка VPN

# 4 Выводы

В ходе выполнения лабораторной работы я получила навыков настройки VPN-туннеля через незащищённое Интернетсоединение.

# 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).

1. 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.

1. 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.

# Список литературы