Отчёт по лабораторной работе №2

Дисциплина: Администрирование локальных сетей

Боровиков Даниил Александрович НПИбд-01-22

Содержание

# 1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

# 2 Задание

1. Сделать предварительную настройку маршрутизатора:

– задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер» (см. пункт 2.5), например msk-donskaya-osbender-gw-1;

– задать интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднять интерфейс;

– задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном);

– настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu);

– сохранить и экспортировать конфигурацию в отдельный файл.

1. Сделать предварительную настройку коммутатора:

– задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер» (см. пункт 2.5), например msk-donskaya-osbender-sw-1;

– задать интерфейсу vlan 2 ip-адрес 192.168.2.1 и маску 255.255.255.0, затем поднять интерфейс;

– привязать интерфейс Fast Ethernet с номером 1 к vlan 2;

– задать в качестве адреса шлюза по умолчанию адрес 192.168.2.254;

– задать пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном);

– настроить доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu);

– для пользователя admin задать доступ 1-го уровня по паролю;

– сохранить и экспортировать конфигурацию в отдельный файл.

# 3 Выполнение лабораторной работы

Создадим проект (рис. 1)

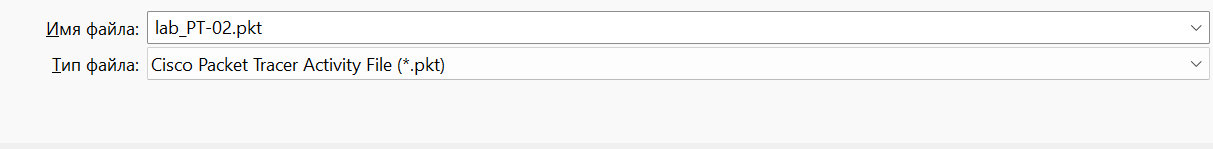


Рис. 1: Создание нового проекта

В логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соединим один PC с маршрутизатором, другой PC — с коммутатором(рис. 2).

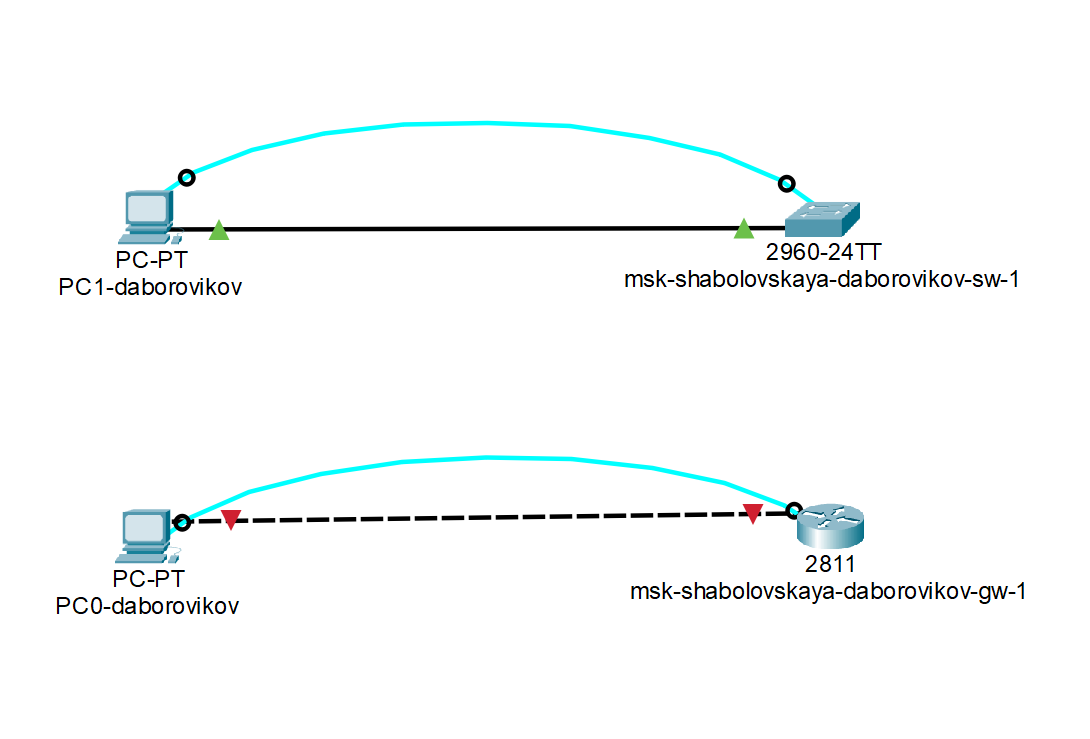


Рис. 2: Схема подключения оборудования для проведения его предварительной настройки

Присвоим статические ip-адреса и маски подсети. (рис. 3).

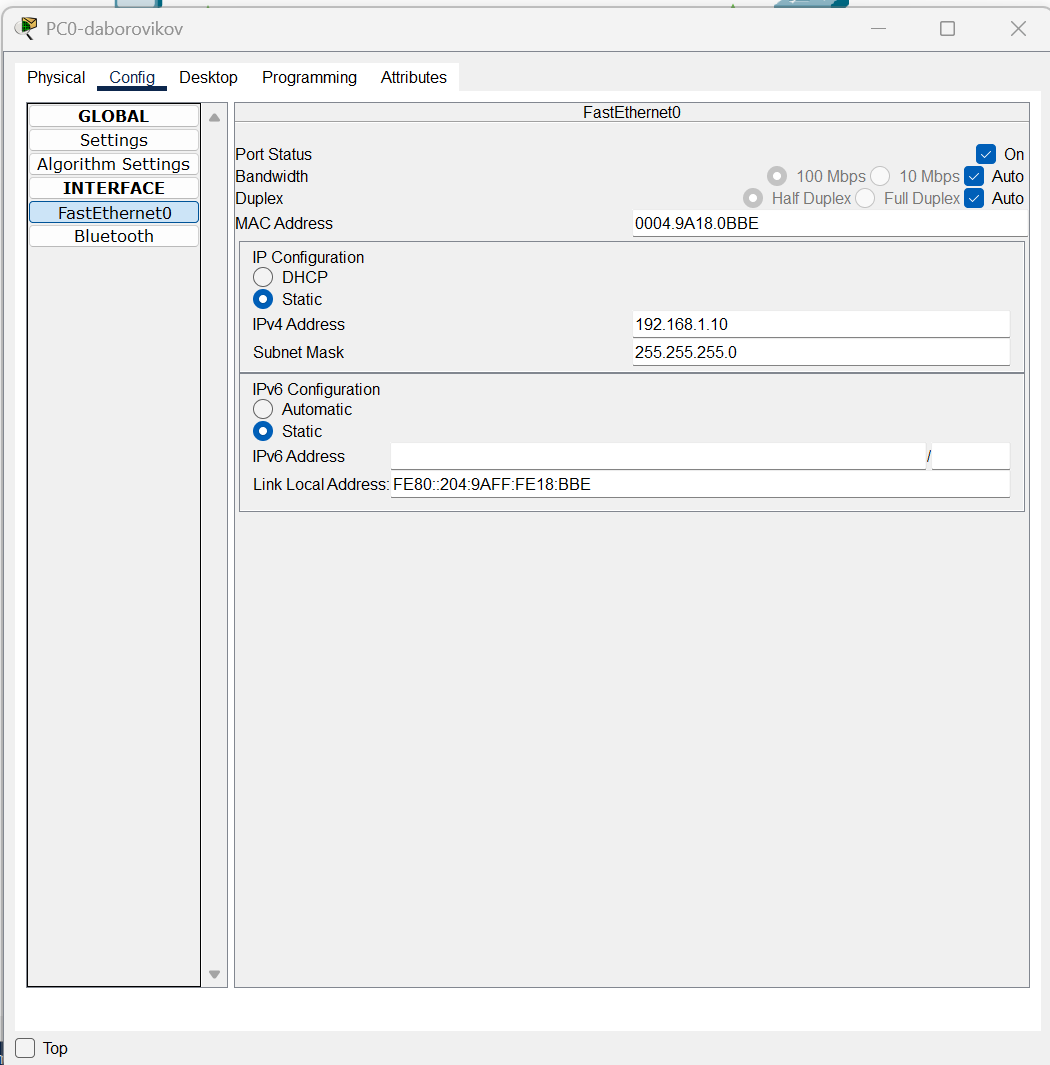


Рис. 3: Статические ip-адреса и маски подсети.

Проведем настройку маршрутизатора в соответствии с заданием(рис. 4).



Рис. 4: Настройка маршрутизатора в соответствии с заданием

Проведем настройку коммутатора в соответствии с заданием(рис. 5).

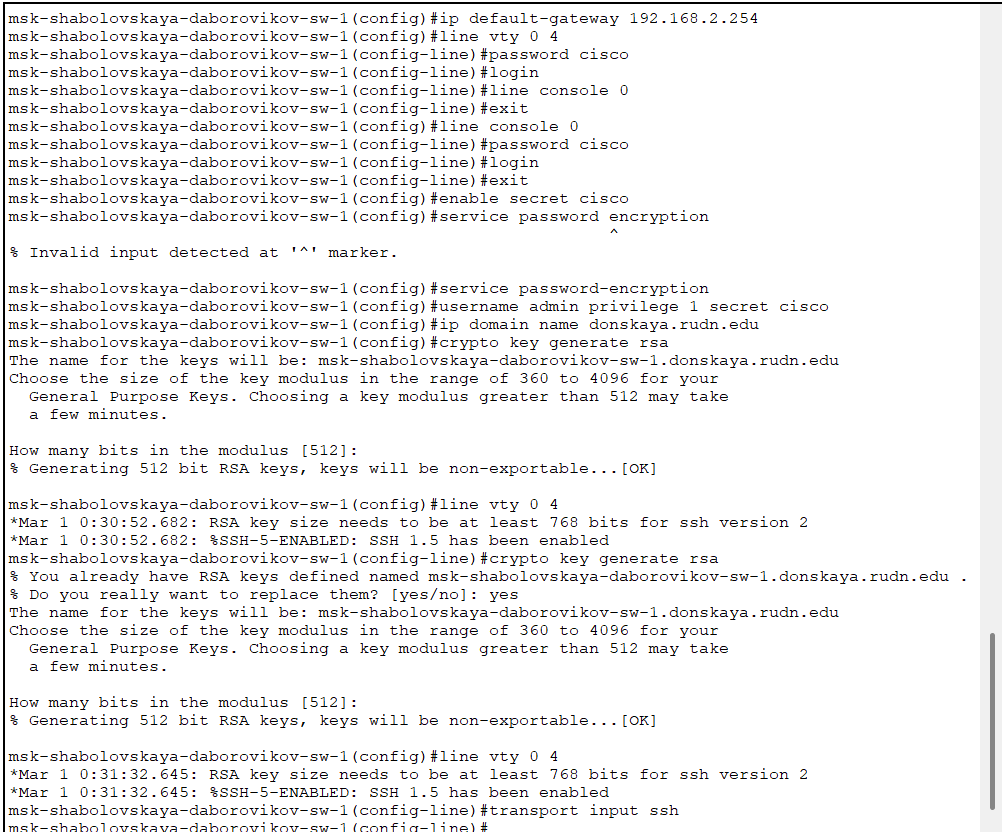


Рис. 5: Настройку коммутатора в соответствии с заданием

Проверьте работоспособность соединений с помощью команды ping на PC0(рис. 6) на PC1 (рис. 7).

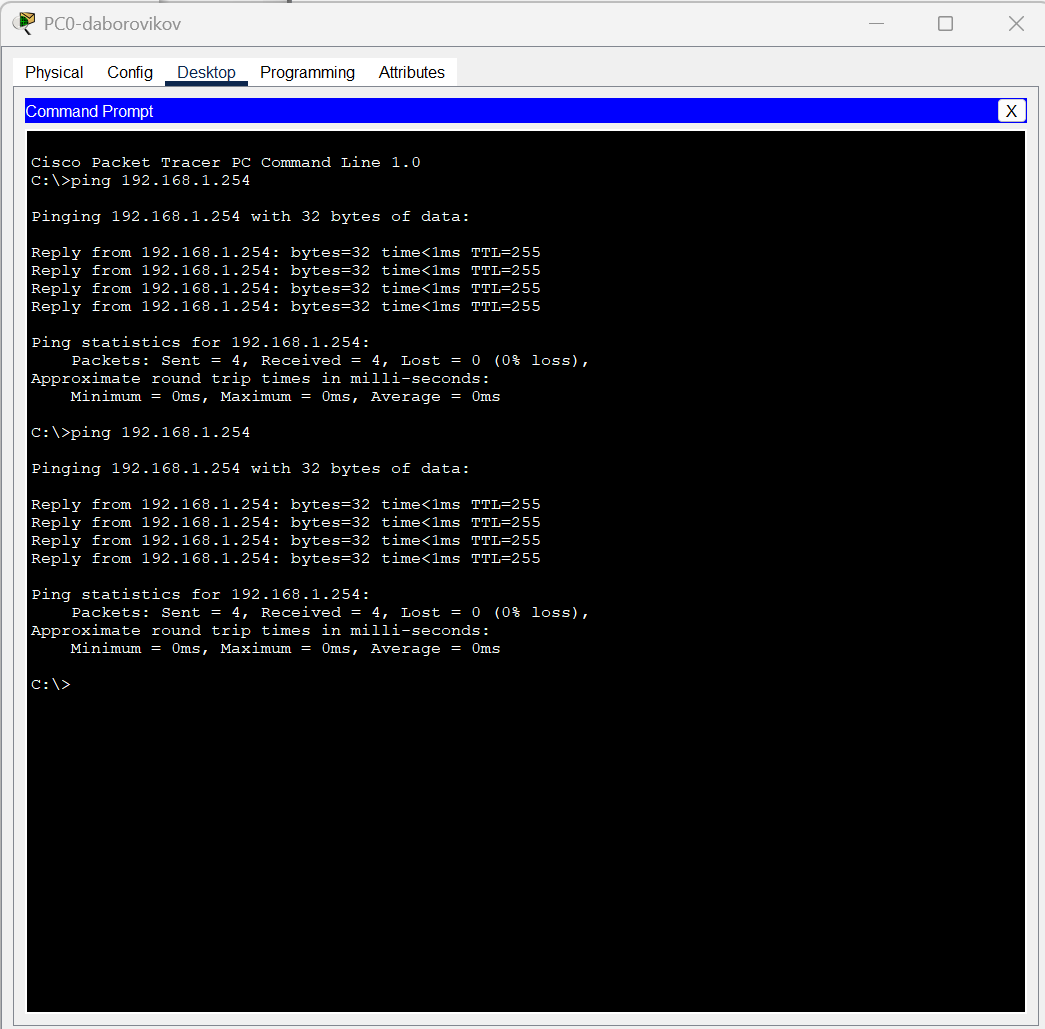


Рис. 6: Проверка работоспособности соединения с помощью команды ping на PC0-daborovikov -> msk-shabolovskaya-daborovikov-gw-1

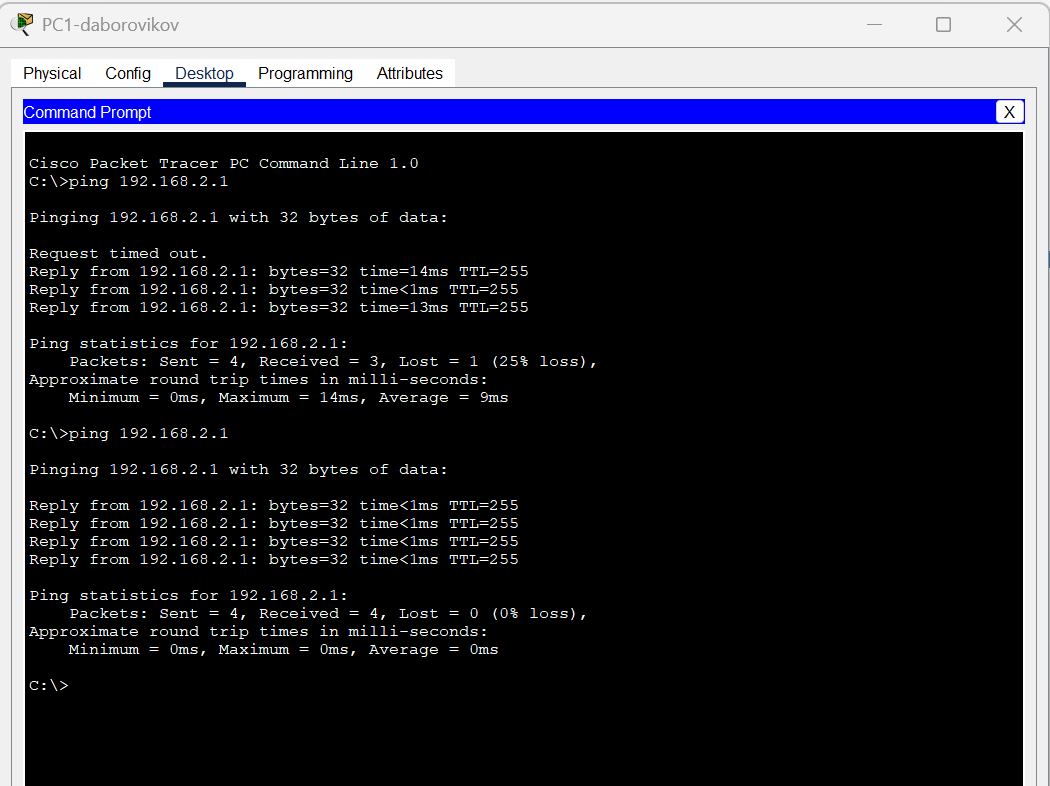


Рис. 7: Проверка работоспособности соединения с помощью команды ping на PC1-daborovikov -> msk-shabolovskaya-daborovikov-sw-1

Попробем подключиться к коммутатору (рис. 9) и маршрутизатору (рис. 8) разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

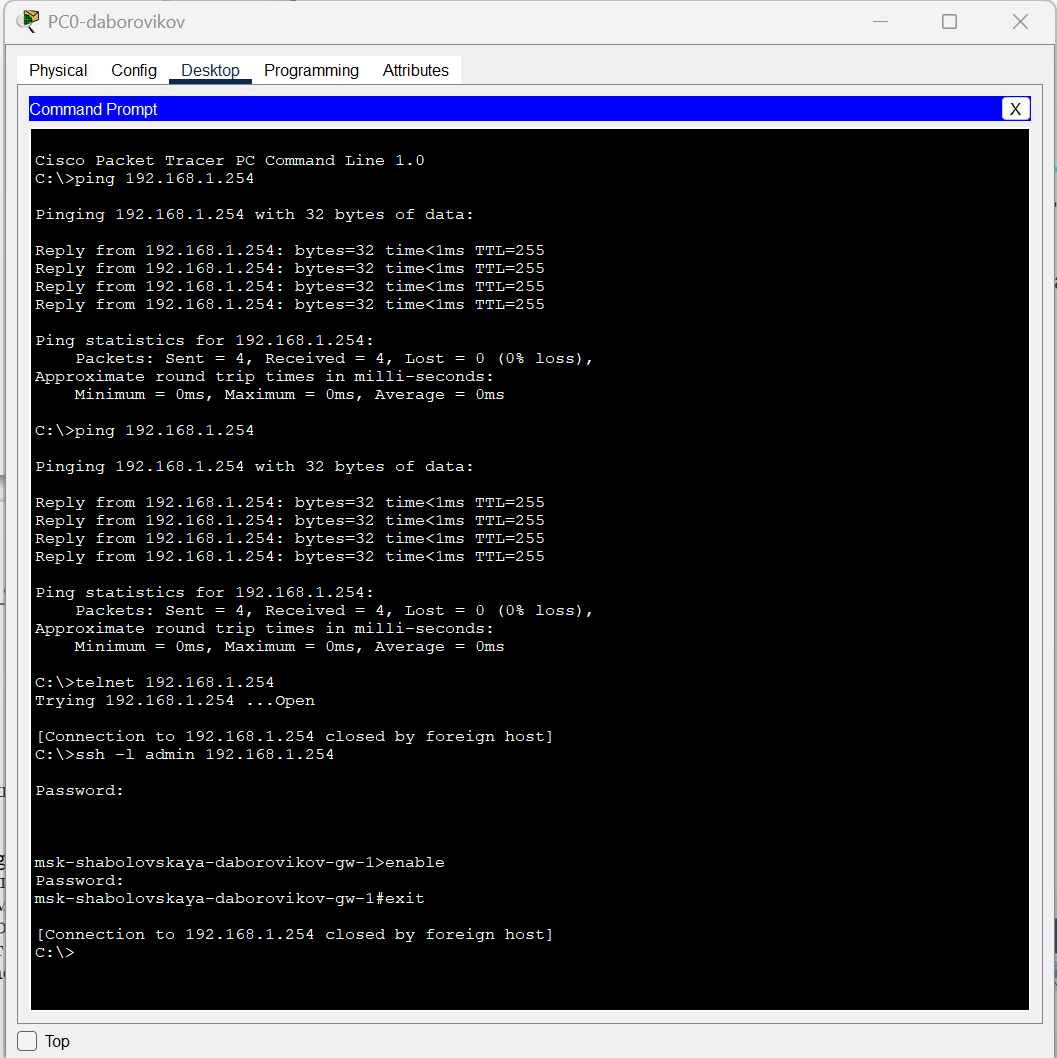


Рис. 8: Попытка подключения к маршрутизатору с помощью консольного кабеля, по протоколу удалённого доступа

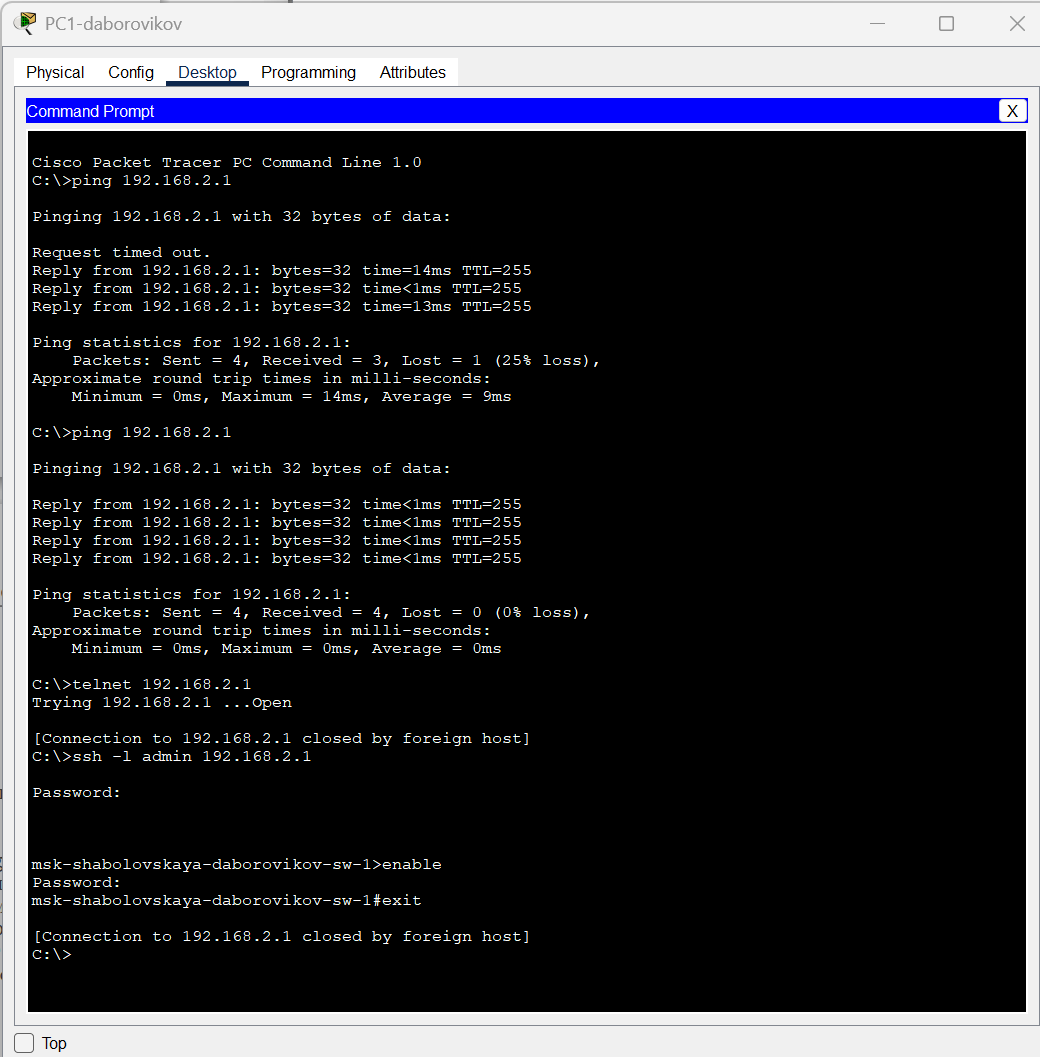


Рис. 9: Попытка подключения к коммутатору с помощью консольного кабеля, по протоколу удалённого доступа

## 3.1 Контрольные вопросы

**1. Укажите возможные способы подключения к сетевому оборудованию.**

* Проводное подключение (Ethernet): наиболее распространенный метод подключения, который использует сетевой кабель (обычно категории Ethernet) для соединения компьютера, маршрутизатора, коммутатора или другого сетевого устройства.
* Беспроводное подключение (Wi-Fi): используют радиоволновые соединения для передачи данных между устройствами. Wi-Fi обычно используется для подключения мобильных устройств, но также может использоваться для подключения компьютеров и другого сетевого оборудования.

**2. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к маршрутизатору и почему?**

* Для подключения оконечного оборудования пользователя к маршрутизатору обычно используется кабель Ethernet. Существует несколько видов Ethernet-кабелей, но наиболее распространенным и рекомендуемым для этой цели является кабель категории 5e (Cat5e) или категории 6 (Cat6).  
  Кабели Cat5e и Cat6 имеют несколько преимуществ, делающих их предпочтительными для подключения оконечного оборудования к маршрутизатору:
* • Скорость и пропускная способность.
* • Поддержка Gigabit Ethernet.
* • Устойчивость к помехам.
* • Будущая совместимость.

**3. Каким типом сетевого кабеля следует подключать оконечное оборудование пользователя к коммутатору и почему?**

* Для подключения оконечного оборудования пользователя к коммутатору также рекомендуется использовать кабель Ethernet. В зависимости от требований сети и возможностей коммутатора, можно использовать кабели различных категорий, но обычно предпочтительными являются кабели категории 5e (Cat5e) или категории 6 (Cat6) по тем же причинам, что и при подключении к маршрутизатору:
* • Скорость и пропускная способность.
* • Поддержка Gigabit Ethernet.
* • Устойчивость к помехам.
* • Будущая совместимость.

**4. Каким типом сетевого кабеля следует подключать коммутатор к коммутатору и почему?**

* Для подключения коммутатора к коммутатору также используются сетевые кабели Ethernet. Однако здесь обычно используются кабели определенной категории в зависимости от требований к сети и пропускной способности, а также от расстояния между коммутаторами. Наиболее распространенными кабелями для соединения коммутаторов являются кабели категории 5e (Cat5e), категории 6 (Cat6) и категории 6a (Cat6a).

Выбор кабеля зависит от нескольких факторов:

• Пропускная способность и расстояние.

• Будущие потребности.

• Бюджет.

• Совместимость с имеющейся инфраструктурой.

Таким образом, для подключения коммутатора к коммутатору наиболее подходящими кабелями являются Cat5e, Cat6 или Cat6a, в зависимости от требований к пропускной способности, расстоянию и бюджету.

**5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю.**

* Пароли на уровне устройства.
* AAA (Authentication, Authorization, Accounting).
* SSH (Secure Shell) или Telnet: SSH и Telnet - это протоколы удаленного управления, которые позволяют администраторам подключаться к сетевому оборудованию через сеть и вводить команды для настройки и управления устройством. Часто они могут быть защищены паролем для обеспечения безопасного доступа.
* Web-based интерфейс управления.
* Локальные аккаунты.
* Протокол SNMP (Simple Network Management Protocol).
* Все эти методы позволяют администраторам обеспечить безопасный доступ к сетевому оборудованию по паролю, минимизируя риски несанкционированного доступа и обеспечивая конфиденциальность и целостность сетевых данных.

**6. Укажите возможные способы настройки удалённого доступа к сетевому оборудованию. Какой из способов предпочтительнее и почему?**

* SSH (Secure Shell): SSH предоставляет защищенное соединение с удаленным сетевым оборудованием через шифрование данных. Этот метод обеспечивает безопасность и конфиденциальность при передаче команд и данных по сети.
* Telnet: Telnet также предоставляет удаленный доступ к сетевому оборудованию, но не обеспечивает защиту данных, так как информация передается в открытом виде. Использование Telnet не рекомендуется из-за небезопасности этого протокола.
* VPN (Virtual Private Network): VPN создает защищенное соединение через общую сеть, такую как интернет, что позволяет удаленным пользователям безопасно подключаться к сетевому оборудованию, как если бы они были внутри локальной сети.
* SSL VPN (Secure Socket Layer Virtual Private Network): SSL VPN предоставляет удаленным пользователям защищенный доступ к сетевому оборудованию через веб-браузер, используя SSL-шифрование для защиты данных.
* Модемный доступ: Многие сетевые устройства могут быть настроены для доступа через модемы, обеспечивая резервное подключение в случае проблем с основной сетью.
* Удаленное управление через веб-интерфейс: Некоторые сетевые устройства предоставляют веб-интерфейс для удаленного управления, который позволяет администраторам настроить и управлять устройством через веб-браузер.

Предпочтительным методом для настройки удаленного доступа к сетевому оборудованию является использование SSH или VPN. Оба эти метода обеспечивают защищенное соединение и шифрование данных, что обеспечивает конфиденциальность и безопасность при удаленном доступе. SSH особенно удобен для доступа к командной строке устройства, в то время как VPN обеспечивает более универсальный и общий доступ к сети. Таким образом, использование SSH или VPN является предпочтительным для обеспечения безопасного удаленного доступа к сетевому оборудованию.

# 4 Выводы

Я приобрел навыки по начальному конфигурированию оборудования Cisco.