

# **Отчёт по лабораторной работе №2**

**Дисциплина: Администрирование локальных сетей**

**Боровиков Даниил Александрович НПИбд-01-22**

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>8</b>
3.1	Контрольные вопросы . . . . .	14
<b>4</b>	<b>Выводы</b>	<b>19</b>

## Список иллюстраций

3.1	Создание нового проекта . . . . .	8
3.2	Схема подключения оборудования для проведения его предвари- тельной настройки . . . . .	8
3.3	Статические ip-адреса и маски подсети. . . . .	9
3.4	Настройка маршрутизатора в соответствии с заданием . . . . .	10
3.5	Настройку коммутатора в соответствии с заданием . . . . .	10
3.6	Проверка работоспособности соединения с помощью команды ping на PC0-daborovikov -> msk-shabolovskaya-daborovikov-gw-1 . . . . .	11
3.7	Проверка работоспособности соединения с помощью команды ping на PC1-daborovikov -> msk-shabolovskaya-daborovikov-sw-1 . . . . .	12
3.8	Попытка подключения к маршрутизатору с помощью консольного кабеля, по протоколу удалённого доступа . . . . .	13
3.9	Попытка подключения к коммутатору с помощью консольного кабе- ля, по протоколу удалённого доступа . . . . .	14

## Список таблиц

# 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 donsкаya.rudn.edu);
- сохранить и экспортировать конфигурацию в отдельный файл.


2. 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 donsкаya.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. 3.1)



Имя файла:	lab_PT-02.pkt
Тип файла:	Cisco Packet Tracer Activity File (*.pkt)

Рис. 3.1: 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. 3.2).

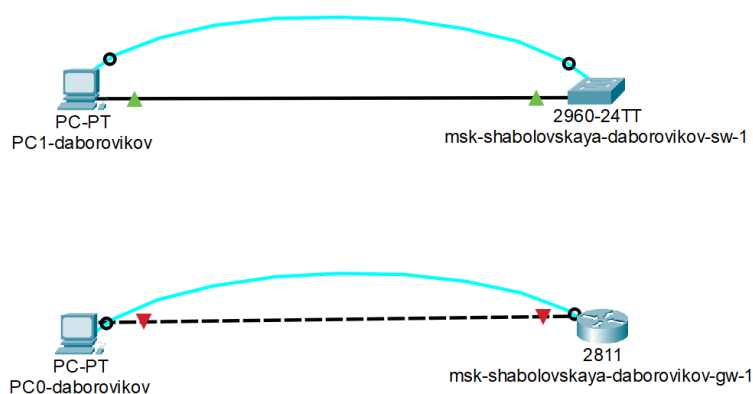


Рис. 3.2: Схема подключения оборудования для проведения его предварительной настройки



Присвоим статические ip-адреса и маски подсети. (рис. 3.3).

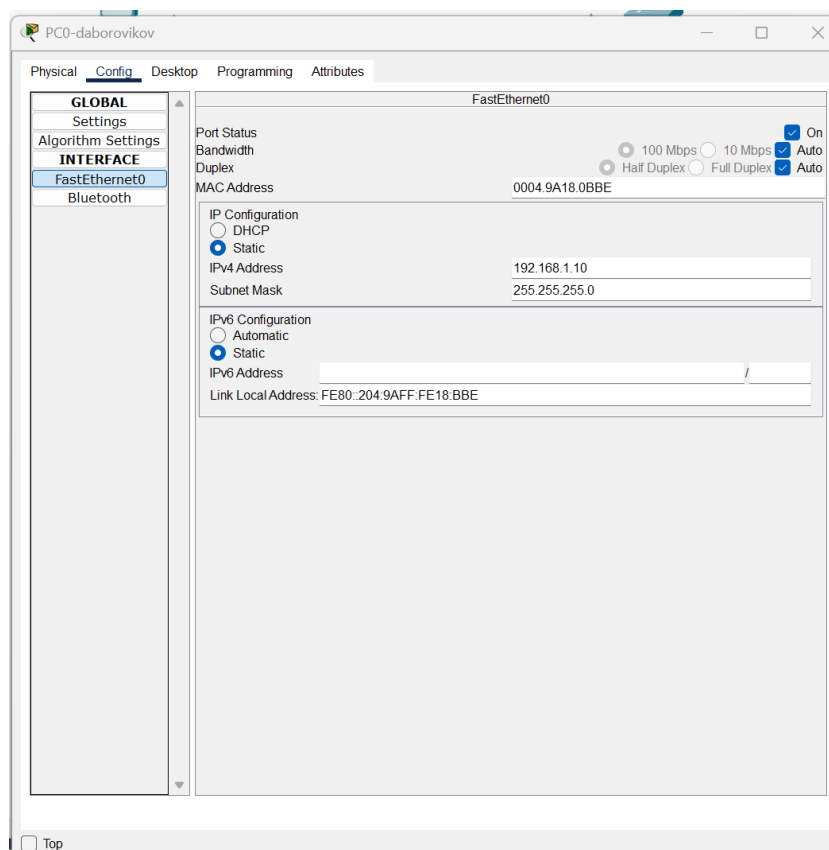


Рис. 3.3: Статические ip-адреса и маски подсети.

Проведем настройку маршрутизатора в соответствии с заданием(рис. 3.4).

```

Router(config)#hostname msk-shabolovskaya-daborovikov-gw-1
msk-shabolovskaya-daborovikov-gw-1(config)#interface f0/0
msk-shabolovskaya-daborovikov-gw-1(config-if)#no shutdown

msk-shabolovskaya-daborovikov-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
ip address 192.168.1.254 255.255.255.0
msk-shabolovskaya-daborovikov-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-shabolovskaya-daborovikov-gw-1(config-if)#no shutdown
msk-shabolovskaya-daborovikov-gw-1(config-if)#exit
msk-shabolovskaya-daborovikov-gw-1(config)#line vty 0 4
msk-shabolovskaya-daborovikov-gw-1(config-line)#password cisco
msk-shabolovskaya-daborovikov-gw-1(config-line)#login
msk-shabolovskaya-daborovikov-gw-1(config-line)#exit
msk-shabolovskaya-daborovikov-gw-1(config)#line console 0
msk-shabolovskaya-daborovikov-gw-1(config-line)#password cisco
msk-shabolovskaya-daborovikov-gw-1(config-line)#login
msk-shabolovskaya-daborovikov-gw-1(config-line)#login
msk-shabolovskaya-daborovikov-gw-1(config-line)#exit
msk-shabolovskaya-daborovikov-gw-1(config)#enable secret cisco
msk-shabolovskaya-daborovikov-gw-1(config)#service password encryption
^
% Invalid input detected at '^' marker.

msk-shabolovskaya-daborovikov-gw-1(config)#service password-encryption
msk-shabolovskaya-daborovikov-gw-1(config)#username admin privilege 1 secret cisco
msk-shabolovskaya-daborovikov-gw-1(config)#ip domain name donskeya.rudn.edu
msk-shabolovskaya-daborovikov-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-shabolovskaya-daborovikov-gw-1.donskeya.rudn.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]

msk-shabolovskaya-daborovikov-gw-1(config)#line vty 0 4
*Mar 1 0:18:27.32: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:18:27.32: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-shabolovskaya-daborovikov-gw-1(config-line)#transport input ssh
msk-shabolovskaya-daborovikov-gw-1(config-line)#

```

Рис. 3.4: Настройка маршрутизатора в соответствии с заданием

Проведем настройку коммутатора в соответствии с заданием(рис. 3.5).

```

msk-shabolovskaya-daborovikov-sw-1(config)#ip default-gateway 192.168.2.254
msk-shabolovskaya-daborovikov-sw-1(config)#line vty 0 4
msk-shabolovskaya-daborovikov-sw-1(config-line)#password cisco
msk-shabolovskaya-daborovikov-sw-1(config-line)#login
msk-shabolovskaya-daborovikov-sw-1(config-line)#line console 0
msk-shabolovskaya-daborovikov-sw-1(config-line)#exit
msk-shabolovskaya-daborovikov-sw-1(config)#line console 0
msk-shabolovskaya-daborovikov-sw-1(config-line)#password cisco
msk-shabolovskaya-daborovikov-sw-1(config-line)#login
msk-shabolovskaya-daborovikov-sw-1(config-line)#exit
msk-shabolovskaya-daborovikov-sw-1(config)#enable secret cisco
msk-shabolovskaya-daborovikov-sw-1(config)#service password encryption
^
% Invalid input detected at '^' marker.

msk-shabolovskaya-daborovikov-sw-1(config)#service password-encryption
msk-shabolovskaya-daborovikov-sw-1(config)#username admin privilege 1 secret cisco
msk-shabolovskaya-daborovikov-sw-1(config)#ip domain name donskeya.rudn.edu
msk-shabolovskaya-daborovikov-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-shabolovskaya-daborovikov-sw-1.donskeya.rudn.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]

msk-shabolovskaya-daborovikov-sw-1(config)#line vty 0 4
*Mar 1 0:30:52.682: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:30:52.682: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-shabolovskaya-daborovikov-sw-1(config-line)#crypto key generate rsa
% You already have RSA keys defined named msk-shabolovskaya-daborovikov-sw-1.donskeya.rudn.edu
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: msk-shabolovskaya-daborovikov-sw-1.donskeya.rudn.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]

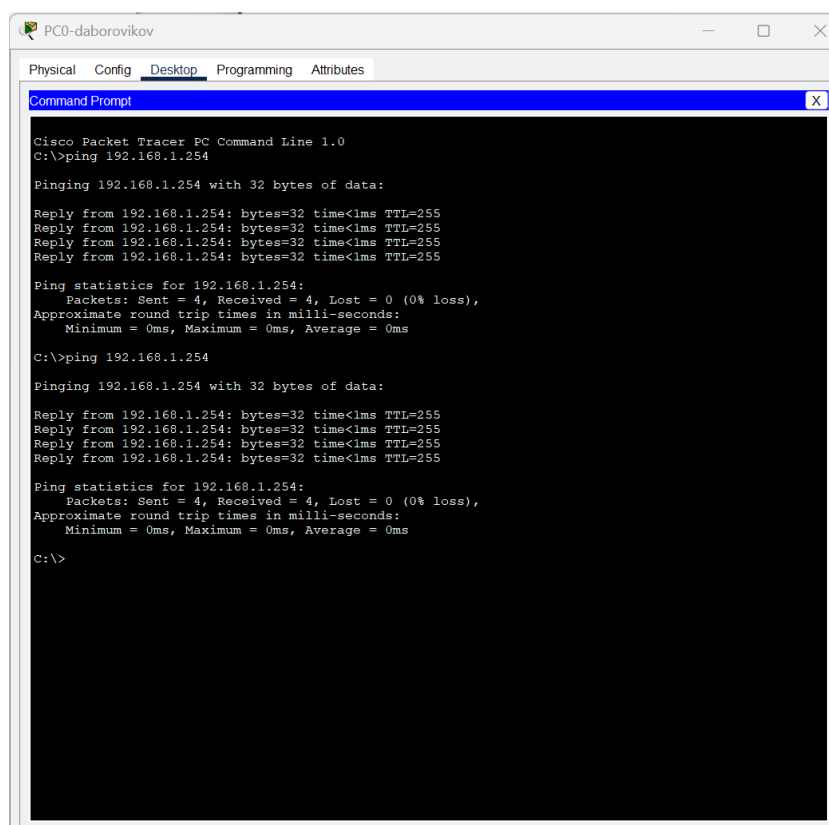
msk-shabolovskaya-daborovikov-sw-1(config)#line vty 0 4
*Mar 1 0:31:32.645: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:31:32.645: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-shabolovskaya-daborovikov-sw-1(config-line)#transport input ssh
msk-shabolovskaya-daborovikov-sw-1(config-line)#

```

Рис. 3.5: Настройку коммутатора в соответствии с заданием

Проверьте работоспособность соединений с помощью команды ping на PC0(рис.

3.6) на PC1 (рис. 3.7).



```
PC0-daborovikov
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.254

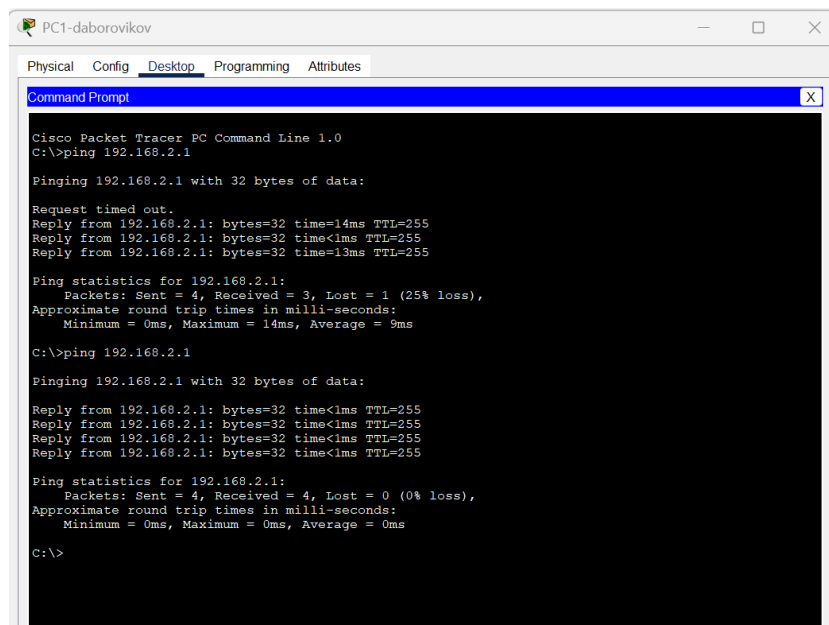
Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рис. 3.6: Проверка работоспособности соединения с помощью команды ping на PC0-daborovikov -> msk-shabolovskaya-daborovikov-gw-1



```
PC1-daborovikov
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.1: bytes=32 time=14ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=13ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 9ms

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рис. 3.7: Проверка работоспособности соединения с помощью команды ping на PC1-daborovikov -> msk-shabolovskaya-daborovikov-sw-1

Попробем подключиться к коммутатору (рис. 3.9) и маршрутизатору (рис. 3.8) разными способами: с помощью консольного кабеля, по протоколу удалённого доступа (telnet, ssh).

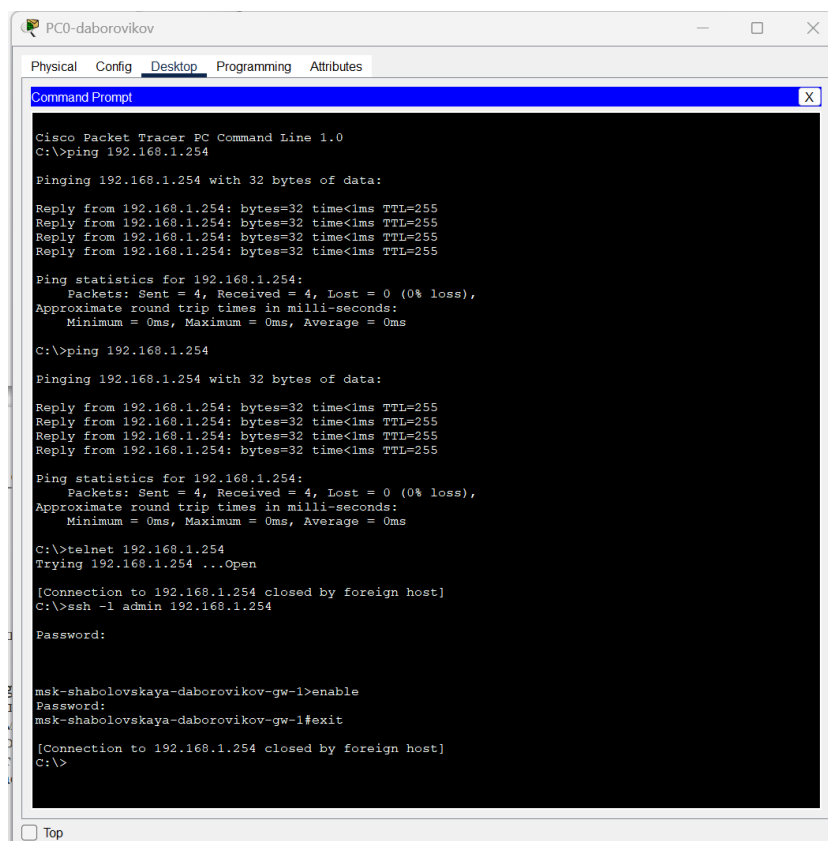


Рис. 3.8: Попытка подключения к маршрутизатору с помощью консольного кабеля, по протоколу удалённого доступа

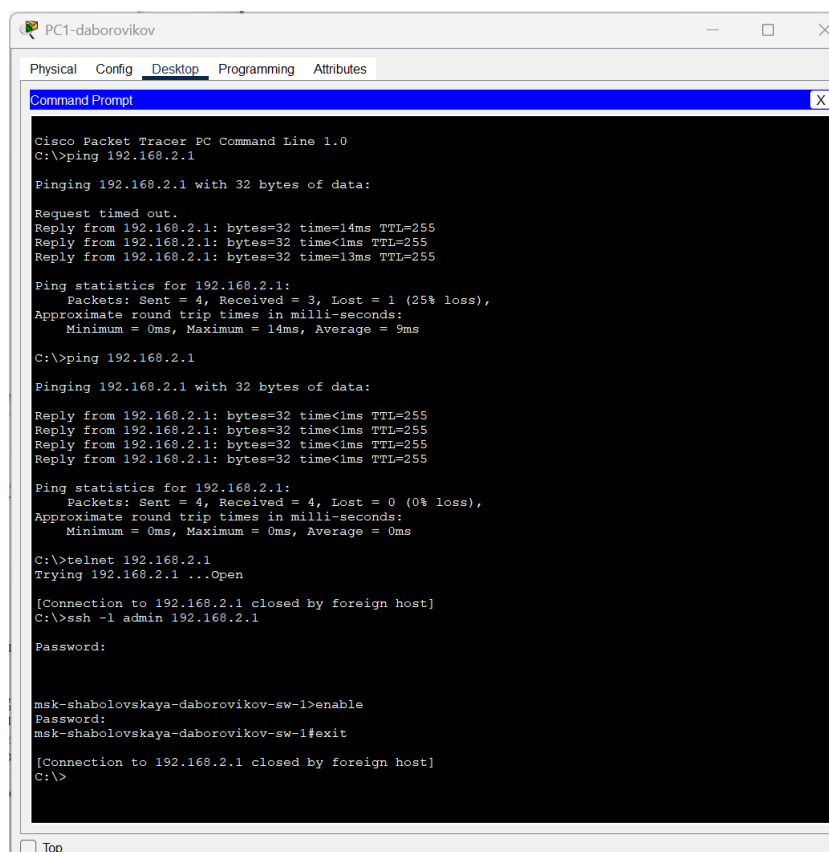


Рис. 3.9: Попытка подключения к коммутатору с помощью консольного кабеля, по протоколу удалённого доступа

## 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 5е (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 5е (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 5е (Cat5e), категории 6 (Cat6) и категории 6а (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.