

Отчёт по лабораторной работе 2

Предварительная настройка оборудования Cisco

Гафоров Нурмухаммад

Содержание

| | |
|---|-----------|
| 1 Введение | 5 |
| 1.1 Цель работы | 5 |
| 2 Ход выполнения | 6 |
| 3 Вывод | 14 |
| 3.1 Контрольные вопросы | 14 |
| 3.1.1 1. Укажите возможные способы подключения к сетевому обо- рудованию. | 14 |
| 3.1.2 2. Каким типом сетевого кабеля следует подключать оконеч- ное оборудование пользователя к маршрутизатору и почему? | 15 |
| 3.1.3 3. Каким типом сетевого кабеля следует подключать оконеч- ное оборудование пользователя к коммутатору и почему? | 15 |
| 3.1.4 4. Каким типом сетевого кабеля следует подключать комму- татор к коммутатору и почему? | 16 |
| 3.1.5 5. Укажите возможные способы настройки доступа к сетевому оборудованию по паролю. | 16 |
| 3.1.6 6. Укажите возможные способы настройки удалённого досту- па к сетевому оборудованию. Какой из способов предпочтите- льнее и почему? | 17 |

Список иллюстраций

| | |
|--|----|
| 2.1 Топология сети: ПК – коммутатор и ПК – маршрутизатор | 6 |
| 2.2 Настройка IP на PC1 | 7 |
| 2.3 Настройка IP на PC0 | 7 |
| 2.4 Конфигурация коммутатора через CLI | 8 |
| 2.5 Завершение настройки SSH на коммутаторе | 9 |
| 2.6 Конфигурация маршрутизатора через CLI | 10 |
| 2.7 Настройка параметров удалённого доступа на маршрутизаторе . . | 11 |
| 2.8 Проверка ping и подключение по SSH к коммутатору | 12 |
| 2.9 Проверка связи и подключение по SSH к маршрутизатору | 13 |

Список таблиц

1 Введение

1.1 Цель работы

Получить основные навыки по начальному конфигурированию оборудования Cisco.

2 Ход выполнения

В логической рабочей области Packet Tracer был создан новый проект. В рабочее поле размещены маршрутизатор **2811**, коммутатор **2960-24ТТ** и два окончных устройства типа **PC-PT**. Один компьютер подключён напрямую к маршрутизатору, второй – к коммутатору. Соединения выполнены медным прямым кабелем (Copper Straight-Through), как показано на схеме.

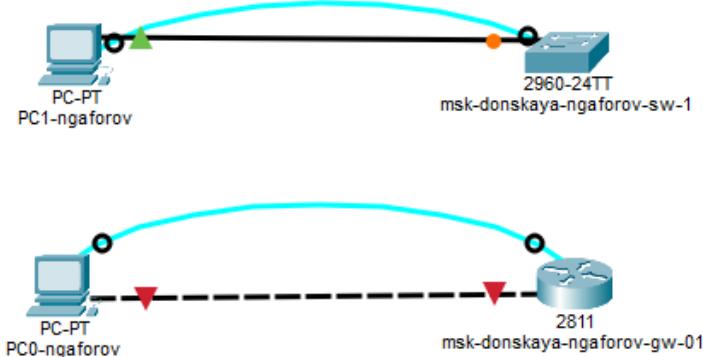


Рис. 2.1: Топология сети: ПК – коммутатор и ПК – маршрутизатор

На первом ПК (подключённом к коммутатору) был задан статический IP-адрес в сети 192.168.2.0/24: - PC1 – **192.168.2.10**

- Маска: **255.255.255.0**
- Основной шлюз: **192.168.2.1**

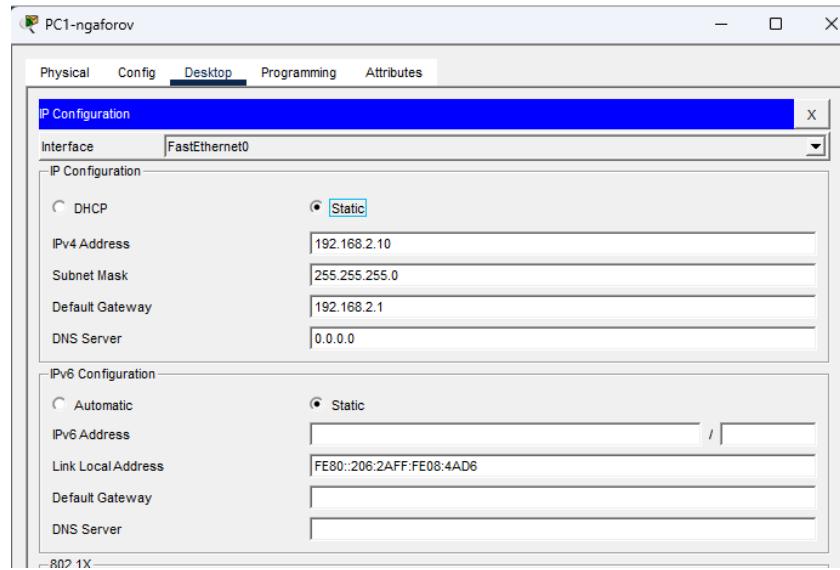


Рис. 2.2: Настройка IP на PC1

На втором ПК (подключённом к маршрутизатору) была настроена адресация сети 192.168.1.0/24: - PC0 – **192.168.1.1**

- Маска: **255.255.255.0**
- Основной шлюз: **192.168.1.254**

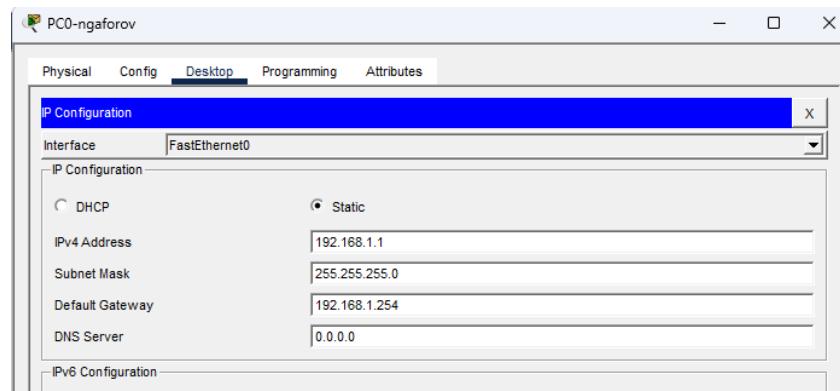
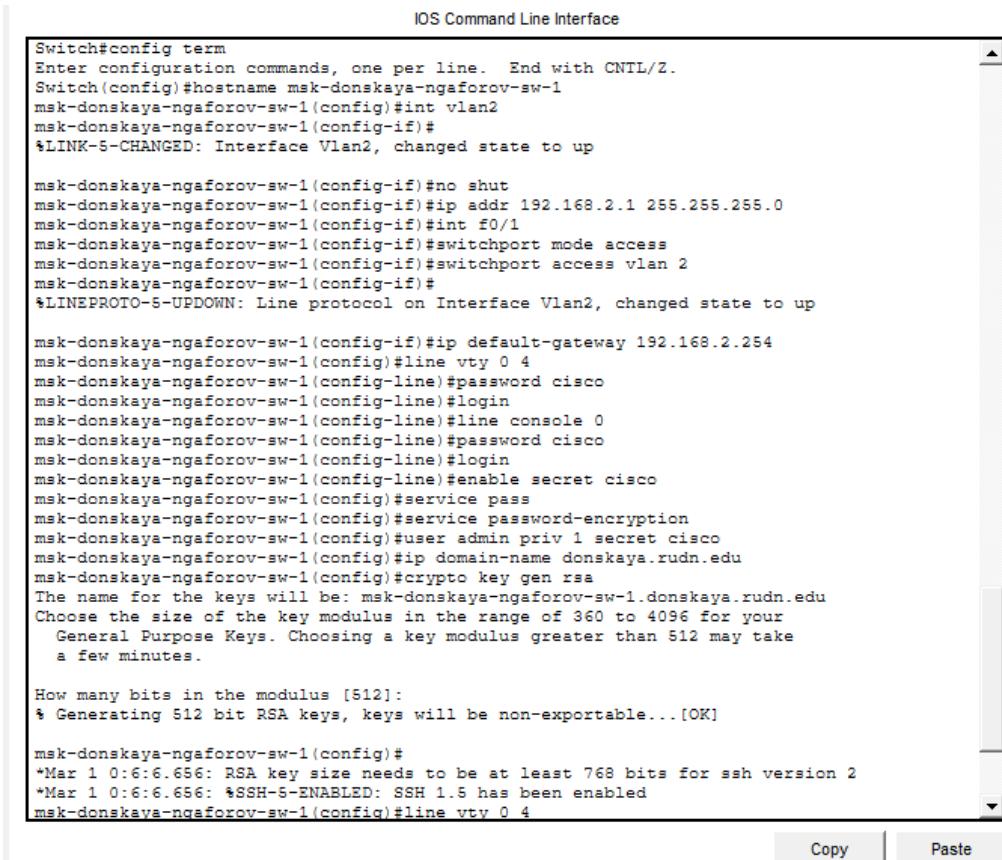


Рис. 2.3: Настройка IP на PC0

На коммутаторе выполнена базовая конфигурация. Установлено имя устройства, создан интерфейс управления VLAN 2 и назначен IP-адрес **192.168.2.1/24**, который используется для удалённого администрирования. Порт FastEthernet0/1 переведён в режим access и привязан к VLAN 2. Также задан шлюз по умолчанию **192.168.2.254**.

Дополнительно настроены параметры доступа: - пароль на консоль и VTY-линии – **cisco**; - включено шифрование паролей; - создан пользователь **admin**; - задан домен; - сгенерированы RSA-ключи; - разрешён доступ по протоколу **SSH**.



The screenshot shows a terminal window titled "IOS Command Line Interface". The command-line interface (CLI) is used to configure a Cisco switch. The configuration includes setting the hostname to "msk-donskaya-ngaforov-sw-1", creating VLAN 2, and setting the IP address to 192.168.2.1. It also configures port 0/1 as an access port for VLAN 2, enables SSH version 2, and generates RSA keys. The "Copy" and "Paste" buttons are visible at the bottom right of the terminal window.

```
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-donskaya-ngaforov-sw-1
msk-donskaya-ngaforov-sw-1(config)#int vlan2
msk-donskaya-ngaforov-sw-1(config-if)#
*LINK-5-CHANGED: Interface Vlan2, changed state to up

msk-donskaya-ngaforov-sw-1(config-if)#no shut
msk-donskaya-ngaforov-sw-1(config-if)#ip addr 192.168.2.1 255.255.255.0
msk-donskaya-ngaforov-sw-1(config-if)#int f0/1
msk-donskaya-ngaforov-sw-1(config-if)#switchport mode access
msk-donskaya-ngaforov-sw-1(config-if)#switchport access vlan 2
msk-donskaya-ngaforov-sw-1(config-if)#
*LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

msk-donskaya-ngaforov-sw-1(config-if)#ip default-gateway 192.168.2.254
msk-donskaya-ngaforov-sw-1(config)#line vty 0 4
msk-donskaya-ngaforov-sw-1(config-line)#password cisco
msk-donskaya-ngaforov-sw-1(config-line)#login
msk-donskaya-ngaforov-sw-1(config-line)#line console 0
msk-donskaya-ngaforov-sw-1(config-line)#password cisco
msk-donskaya-ngaforov-sw-1(config-line)#login
msk-donskaya-ngaforov-sw-1(config-line)#enable secret cisco
msk-donskaya-ngaforov-sw-1(config)#service password-encryption
msk-donskaya-ngaforov-sw-1(config)#user admin priv 1 secret cisco
msk-donskaya-ngaforov-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-ngaforov-sw-1(config)#crypto key gen rsa
The name for the keys will be: msk-donskaya-ngaforov-sw-1.donskaya.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-donskaya-ngaforov-sw-1(config)#
*Mar 1 0:6:6.656: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:6:6.656: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-ngaforov-sw-1(config)#line vty 0 4
```

Рис. 2.4: Конфигурация коммутатора через CLI

```
Switch#config term
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-donskaya-ngaforov-sw-1
msk-donskaya-ngaforov-sw-1(config)#int vlan2
msk-donskaya-ngaforov-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

msk-donskaya-ngaforov-sw-1(config-if)#no shut
msk-donskaya-ngaforov-sw-1(config-if)#ip addr 192.168.2.1 255.255.255.0
msk-donskaya-ngaforov-sw-1(config-if)#int f0/1
msk-donskaya-ngaforov-sw-1(config-if)#switchport mode access
msk-donskaya-ngaforov-sw-1(config-if)#switchport access vlan 2
msk-donskaya-ngaforov-sw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

msk-donskaya-ngaforov-sw-1(config-if)#ip default-gateway 192.168.2.254
msk-donskaya-ngaforov-sw-1(config)#line vty 0 4
msk-donskaya-ngaforov-sw-1(config-line)#password cisco
msk-donskaya-ngaforov-sw-1(config-line)#login
msk-donskaya-ngaforov-sw-1(config-line)#line console 0
msk-donskaya-ngaforov-sw-1(config-line)#password cisco
msk-donskaya-ngaforov-sw-1(config-line)#login
msk-donskaya-ngaforov-sw-1(config-line)#enable secret cisco
msk-donskaya-ngaforov-sw-1(config)#service password-encryption
msk-donskaya-ngaforov-sw-1(config)#user admin priv 1 secret cisco
msk-donskaya-ngaforov-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-ngaforov-sw-1(config)#crypto key gen rsa
The name for the keys will be: msk-donskaya-ngaforov-sw-1.donskaya.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-donskaya-ngaforov-sw-1(config)#
*Mar 1 0:6:6.656: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:6:6.656: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-ngaforov-sw-1(config)#line vty 0 4
msk-donskaya-ngaforov-sw-1(config-line)#transport input ssh
msk-donskaya-ngaforov-sw-1(config-line)#

```

Рис. 2.5: Завершение настройки SSH на коммутаторе

На маршрутизаторе настроен интерфейс FastEthernet0/0 с адресом **192.168.1.254/24**, который используется в качестве шлюза для подключённого ПК. Интерфейс активирован командой **no shutdown**.

Также выполнены настройки удалённого доступа: - заданы пароли на консоль и VTY-линии; - включено шифрование паролей; - создан пользователь **admin**; - указан домен; - сгенерированы RSA-ключи; - разрешено подключение по **SSH**.

```
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname msk-donskaya-gw-ngaforov-01
msk-donskaya-gw-ngaforov-01(config)#int F0/0
msk-donskaya-gw-ngaforov-01(config-if)#no shut

msk-donskaya-gw-ngaforov-01(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

msk-donskaya-gw-ngaforov-01(config-if)#ip address 192.168.1.254 255.255.255.0
msk-donskaya-gw-ngaforov-01(config-if)#line vty 0 4
msk-donskaya-gw-ngaforov-01(config-line)#password cisco
msk-donskaya-gw-ngaforov-01(config-line)#login
msk-donskaya-gw-ngaforov-01(config-line)#line console 0
msk-donskaya-gw-ngaforov-01(config-line)#password cisco
msk-donskaya-gw-ngaforov-01(config-line)#login
msk-donskaya-gw-ngaforov-01(config-line)#enable secret cisco
msk-donskaya-gw-ngaforov-01(config)#service password-encryption
msk-donskaya-gw-ngaforov-01(config)#user admin priv 1 secret cisco
msk-donskaya-gw-ngaforov-01(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-gw-ngaforov-01(config)#crypto key gen rsa
The name for the keys will be: msk-donskaya-gw-ngaforov-01.donskaya.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-donskaya-gw-ngaforov-01(config)#line vty 0 4
*Mar 1 0:12:31.595: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:12:31.595: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-gw-ngaforov-01(config-line)#transport input ssh
msk-donskaya-gw-ngaforov-01(config-line)#
msk-donskaya-gw-ngaforov-01#
%SYS-5-CONFIG_I: Configured from console by console
```

Рис. 2.6: Конфигурация маршрутизатора через CLI

```

Router>enable
Router#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname msk-donskaya-gw-ngaforov-01
msk-donskaya-gw-ngaforov-01(config)#int f0/0
msk-donskaya-gw-ngaforov-01(config-if)#no shut

msk-donskaya-gw-ngaforov-01(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

msk-donskaya-gw-ngaforov-01(config-if)#ip address 192.168.1.254 255.255.255.0
msk-donskaya-gw-ngaforov-01(config-if)#line vty 0 4
msk-donskaya-gw-ngaforov-01(config-line)#password cisco
msk-donskaya-gw-ngaforov-01(config-line)#login
msk-donskaya-gw-ngaforov-01(config-line)#line console 0
msk-donskaya-gw-ngaforov-01(config-line)#password cisco
msk-donskaya-gw-ngaforov-01(config-line)#login
msk-donskaya-gw-ngaforov-01(config-line)#enable secret cisco
msk-donskaya-gw-ngaforov-01(config)#service password-encryption
msk-donskaya-gw-ngaforov-01(config)#user admin priv 1 secret cisco
msk-donskaya-gw-ngaforov-01(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-gw-ngaforov-01(config)#crypto key gen rsa
The name for the keys will be: msk-donskaya-gw-ngaforov-01.donskaya.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-donskaya-gw-ngaforov-01(config)#line vty 0 4
*Mar 1 0:12:31.595: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:12:31.595: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-gw-ngaforov-01(config-line)#transport in ssh
msk-donskaya-gw-ngaforov-01(config-line)#
msk-donskaya-gw-ngaforov-01#
%SYS-5-CONFIG_I: Configured from console by console

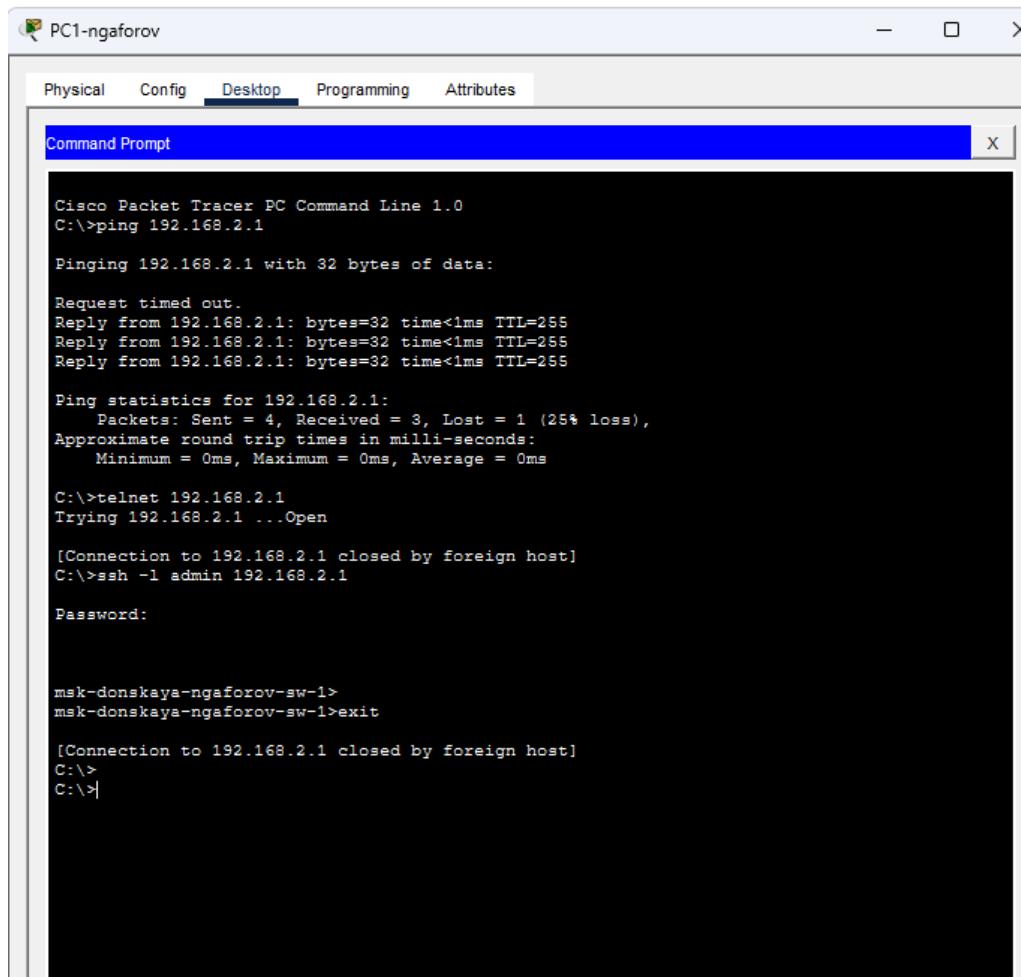
```

Рис. 2.7: Настройка параметров удалённого доступа на маршрутизаторе

После завершения настройки была выполнена проверка доступности устройств с помощью команды **ping**.

С ПК, подключённого к коммутатору, была проверена доступность IP-адреса коммутатора **192.168.2.1**. Ответы получены, что подтверждает корректную настройку сети.

Далее была выполнена попытка удалённого подключения: - по **telnet** – соединение устанавливается, но закрывается; - по **SSH** – выполнен успешный вход под пользователем **admin**.



The screenshot shows a window titled "PC1-ngaforov" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is selected. Inside the window, there is a "Command Prompt" window with the following text:

```
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<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 = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:>telnet 192.168.2.1
Trying 192.168.2.1 ...Open

[Connection to 192.168.2.1 closed by foreign host]
C:>ssh -l admin 192.168.2.1

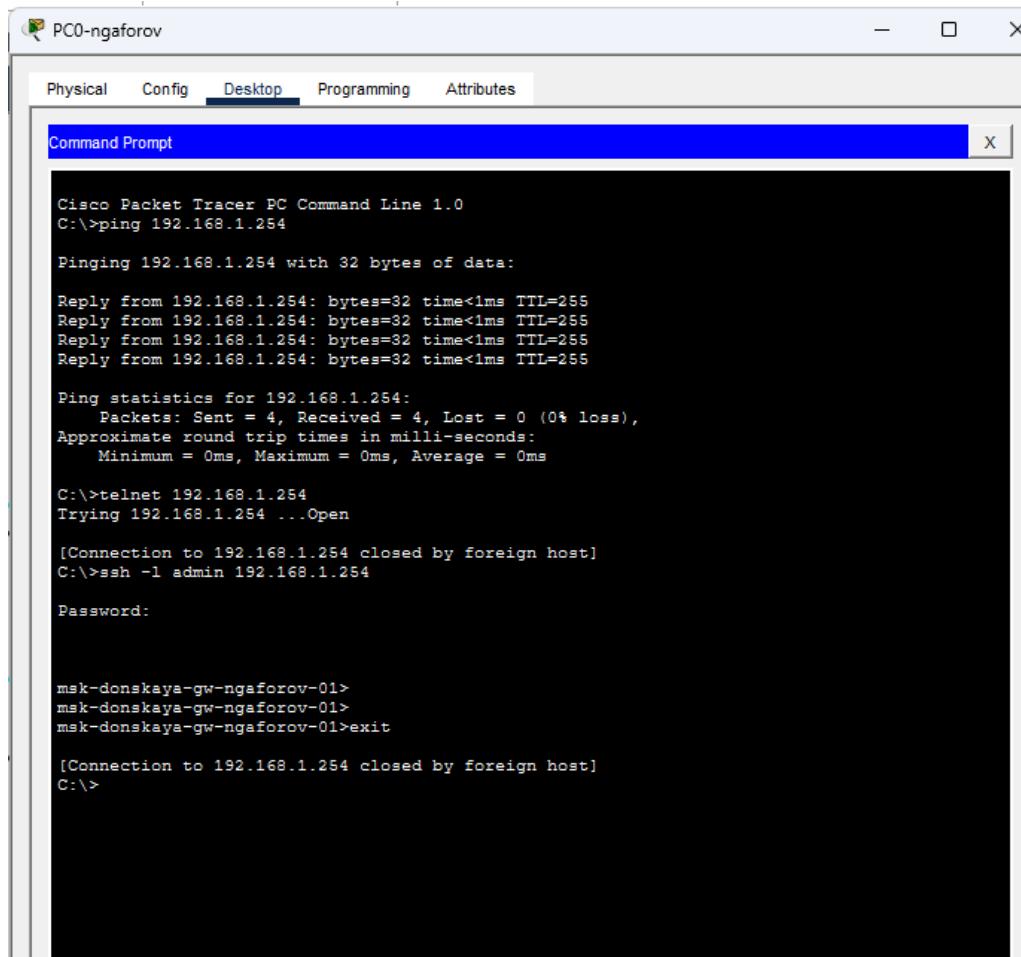
Password:

msk-donskaya-ngaforov-sw-1>
msk-donskaya-ngaforov-sw-1>exit

[Connection to 192.168.2.1 closed by foreign host]
C:>
C:>
```

Рис. 2.8: Проверка ping и подключение по SSH к коммутатору

Аналогичная проверка была выполнена с ПК, подключённого к маршрутизатору. Выполнен ping до адреса **192.168.1.254**, получены ответы без потерь пакетов. Затем выполнено подключение по SSH, подтверждающее корректную настройку удалённого администрирования.



The screenshot shows a window titled "PC0-ngaforov" with a tab bar containing "Physical", "Config", "Desktop", "Programming", and "Attributes". The "Desktop" tab is selected. Below the tabs is a title bar for "Command Prompt" with a close button. The main area displays the following command-line session:

```
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

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:\>telnet 192.168.1.254
Trying 192.168.1.254 ...Open

[Connection to 192.168.1.254 closed by foreign host]
C:\>ssh -l admin 192.168.1.254

Password:

msk-donskaya-gw-ngaforov-01>
msk-donskaya-gw-ngaforov-01>
msk-donskaya-gw-ngaforov-01>exit

[Connection to 192.168.1.254 closed by foreign host]
C:\>
```

Рис. 2.9: Проверка связи и подключение по SSH к маршрутизатору

В результате выполнения работы была создана и настроена простая сеть с использованием маршрутизатора и коммутатора. Проведена базовая конфигурация устройств, назначены IP-адреса, настроены параметры удалённого доступа и выполнена проверка связности с помощью ICMP-пакетов и протокола SSH.

3 Вывод

В ходе выполнения работы была создана и настроена простая сеть в Cisco Packet Tracer с использованием маршрутизатора, коммутатора и двух оконечных устройств. Выполнена базовая конфигурация сетевого оборудования: назначены IP-адреса интерфейсам, настроены параметры управления коммутатором через VLAN, задан шлюз по умолчанию и активированы интерфейсы. Были отработаны навыки настройки удалённого доступа к сетевым устройствам. Настроены линии console и VTY, включено шифрование паролей, создан локальный пользователь, сгенерированы RSA-ключи и выполнена настройка подключения по протоколу SSH. Проведена проверка доступности устройств с помощью команды ping, что подтвердило корректность выполненной адресации и соединений. Также была выполнена попытка подключения к маршрутизатору и коммутатору различными способами: через консольный кабель, а также по протоколам удалённого доступа telnet и SSH. Установлено, что защищённое подключение по SSH обеспечивает успешный удалённый вход на устройства и позволяет управлять ими по сети.

3.1 Контрольные вопросы

3.1.1 1. Укажите возможные способы подключения к сетевому оборудованию.

Существует несколько способов подключения к сетевым устройствам для их настройки и администрирования:

- **Консольное подключение** — прямое соединение компьютера с устройством через консольный кабель. Используется для первоначальной настройки.
- **Telnet** — удалённое подключение по сети с передачей данных в открытом виде.
- **SSH** — удалённое защищённое подключение с шифрованием данных.
- **Web-интерфейс** — доступ через браузер (если поддерживается устройством).
- **Через вспомогательный (AUX) порт** — используется реже, обычно для удалённого доступа через модем.

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

Оконечное оборудование подключается к маршрутизатору с помощью **прямого медного кабеля (Copper Straight-Through)**.

Это связано с тем, что соединяются устройства разного типа: - компьютер (оконечное устройство); - маршрутизатор (сетевое устройство).

У таких устройств используются разные схемы передачи и приёма сигналов, поэтому прямой кабель обеспечивает корректное соединение.

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

Для подключения ПК к коммутатору также используется **прямой медный кабель (Copper Straight-Through)**.

Коммутатор является промежуточным сетевым устройством, а компьютер —

оконечным. Поскольку соединяются разные типы устройств, применяется прямой кабель, обеспечивающий правильное соответствие контактов передачи и приёма.

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

Для соединения двух коммутаторов традиционно используется **перекрёстный кабель (Copper Cross-Over)**.

Это объясняется тем, что соединяются однотипные устройства. У них одинаковое расположение линий передачи и приёма, поэтому требуется перекрёстное соединение контактов для корректной передачи данных. В современных устройствах часто применяется технология Auto-MDIX, которая позволяет использовать и прямой кабель.

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

Доступ к сетевому оборудованию можно защитить несколькими способами:

- установка пароля на **console line** — для локального доступа через консоль;
- установка пароля на **VTY-линии** — для удалённых подключений;
- использование команды **enable secret** — для защиты привилегированного режима;
- создание локального пользователя с именем и паролем;
- включение шифрования паролей с помощью **service password-encryption**.

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

Удалённый доступ можно настроить следующими способами:

- **Telnet** – простой способ удалённого подключения по сети;
- **SSH** – защищённое подключение с использованием шифрования.

Предпочтительным является **SSH**, так как он шифрует передаваемые данные, включая логины и пароли. В отличие от Telnet, который передаёт информацию в открытом виде, SSH обеспечивает более высокий уровень безопасности и защиты от перехвата данных.