

# **Отчёт по лабораторной работе №2**

**Предварительная настройка оборудования Cisco**

Владимир Базлов

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение</b>	<b>6</b>
2.1 Настройка маршрутизатора и коммутатора с проверкой удалённого доступа . . . . .	6
<b>3 Контрольные вопросы</b>	<b>14</b>
<b>4 Заключение</b>	<b>17</b>

# **Список иллюстраций**

2.1 Схема подключения ПК к маршрутизатору и коммутатору . . . . .	7
2.2 Настройка IP-адреса PC1 . . . . .	8
2.3 Настройка IP-адреса PC0 . . . . .	8
2.4 Настройка маршрутизатора через CLI . . . . .	9
2.5 Консольный доступ и команды настройки маршрутизатора . . . . .	10
2.6 Настройка коммутатора через CLI . . . . .	11
2.7 Ping и удалённый доступ к маршрутизатору (Telnet/SSH) . . . . .	12
2.8 Ping и удалённый доступ к коммутатору (Telnet/SSH) . . . . .	13

# **Список таблиц**

# **1 Цель работы**

Получить основные навыки по начальному конфигурированию оборудования Cisco.

## **2 Выполнение**

### **2.1 Настройка маршрутизатора и коммутатора с проверкой удалённого доступа**

1. В логической рабочей области Cisco Packet Tracer размещены устройства: маршрутизатор **2911**, коммутатор **2960-24TT** и два оконечных устройства **PC-PT**.

Один компьютер подключён к маршрутизатору с помощью медного прямого кабеля, второй – к коммутатору. Таким образом сформированы два сегмента сети, обеспечивающие доступ к сетевым устройствам для последующей настройки и администрирования.

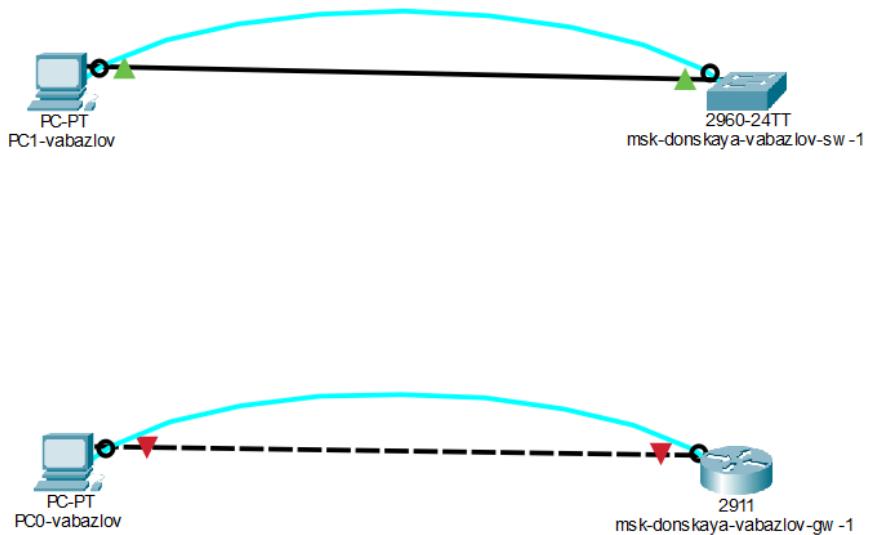


Рис. 2.1: Схема подключения ПК к маршрутизатору и коммутатору

2. На компьютерах выполнена ручная настройка IP-адресов через вкладку **Desktop → IP Configuration.**

Для ПК, подключённого к коммутатору:

- PC1-vabazlov – IP-адрес: 192.168.2.10
- Маска подсети: 255.255.255.0
- Основной шлюз: 192.168.2.1
- DNS: 0.0.0.0

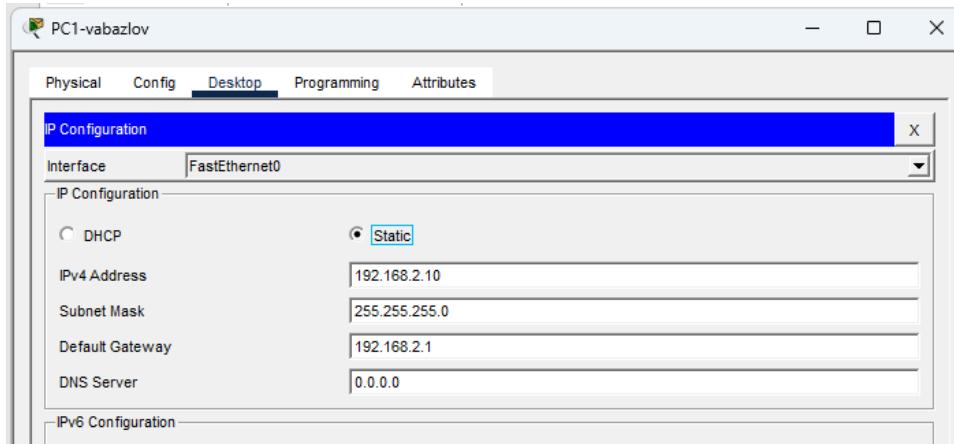


Рис. 2.2: Настройка IP-адреса PC1

Для ПК, подключённого к маршрутизатору:

- PC0-vabazlov – IP-адрес: 192.168.1.10
- Маска подсети: 255.255.255.0
- Основной шлюз: 192.168.1.254
- DNS: 0.0.0.0

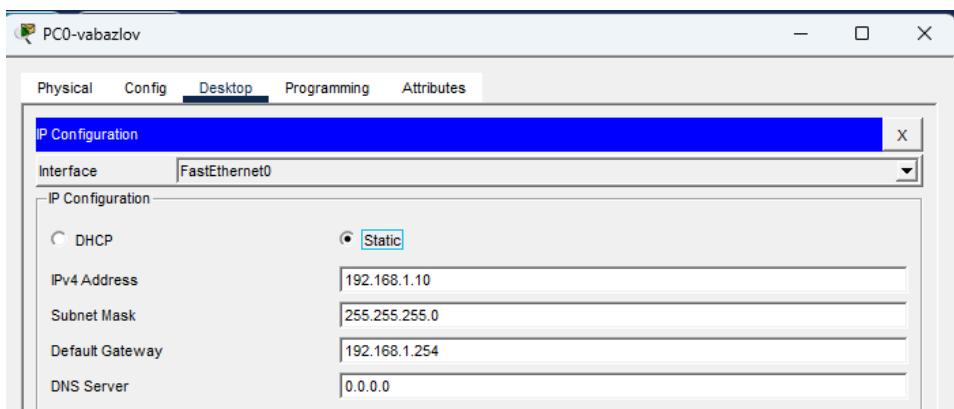


Рис. 2.3: Настройка IP-адреса PC0

3. Выполнена базовая настройка маршрутизатора **msk-donskaya-vabazlov-gw-1** через интерфейс командной строки (**CLI**).

На интерфейсе **GigabitEthernet0/0** задан IP-адрес **192.168.1.254/24** и выполнено включение интерфейса командой **no shutdown**.

Дополнительно настроены параметры удалённого доступа:

- настроены линии VTY (0–4) и включён вход по паролю;
- задан пароль для привилегированного режима (enable);
- создан локальный пользователь **admin** с уровнем привилегий 1;
- задано доменное имя для генерации ключей;
- сгенерированы RSA-ключи;
- включён доступ по SSH и разрешён только SSH на VTY;
- конфигурация сохранена в NVRAM командой **wr mem**.

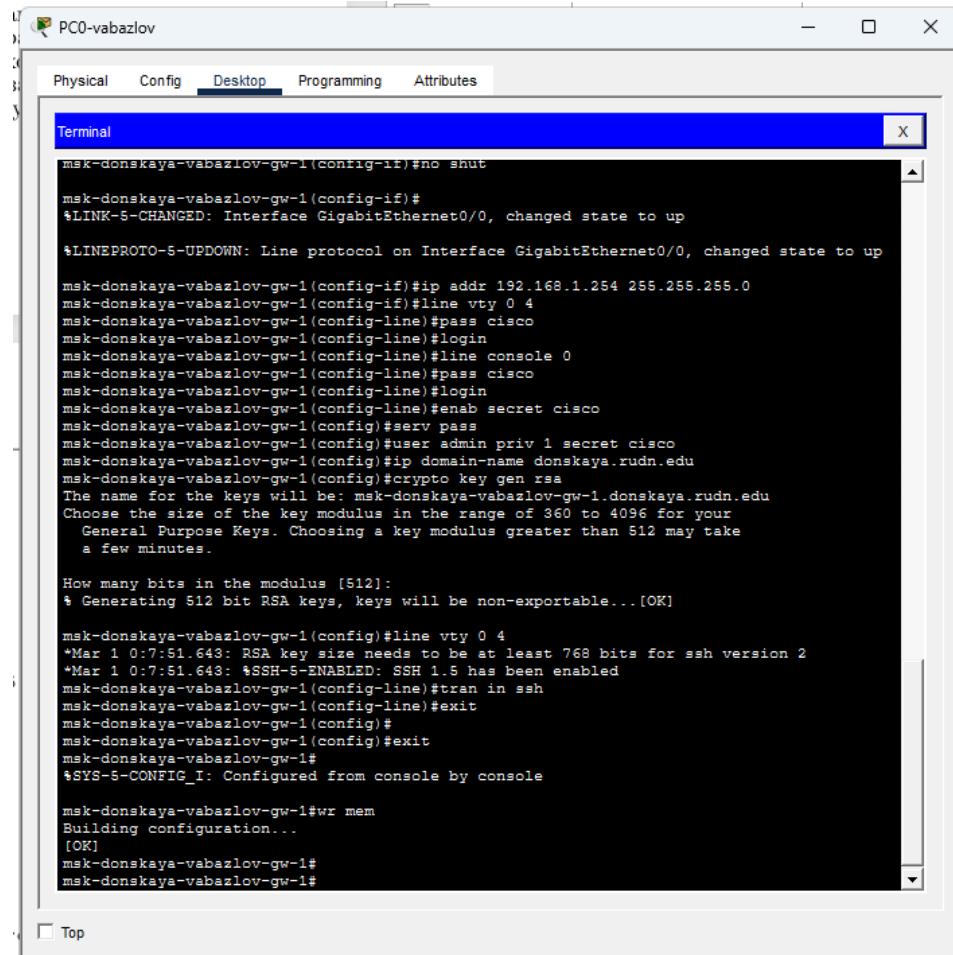
```
msk-donskaya-vabazlov-gw-1(config-if)#  
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up  
  
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up  
  
msk-donskaya-vabazlov-gw-1(config-if)#ip addr 192.168.1.254 255.255.255.0  
msk-donskaya-vabazlov-gw-1(config-if)#line vty 0 4  
msk-donskaya-vabazlov-gw-1(config-line)#pass cisco  
msk-donskaya-vabazlov-gw-1(config-line)#login  
msk-donskaya-vabazlov-gw-1(config-line)#line console 0  
msk-donskaya-vabazlov-gw-1(config-line)#pass cisco  
msk-donskaya-vabazlov-gw-1(config-line)#login  
msk-donskaya-vabazlov-gw-1(config-line)#enab secret cisco  
msk-donskaya-vabazlov-gw-1(config)#serv pass  
msk-donskaya-vabazlov-gw-1(config)#user admin priv 1 secret cisco  
msk-donskaya-vabazlov-gw-1(config)#ip domain-name donskaya.rudn.edu  
msk-donskaya-vabazlov-gw-1(config)#crypto key gen rsa  
The name for the keys will be: msk-donskaya-vabazlov-gw-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-vabazlov-gw-1(config)#line vty 0 4  
*Mar 1 0:7:51.643: RSA key size needs to be at least 768 bits for ssh version 2  
*Mar 1 0:7:51.643: %SSH-5-ENABLED: SSH 1.5 has been enabled  
msk-donskaya-vabazlov-gw-1(config-line)#tran in ssh  
msk-donskaya-vabazlov-gw-1(config-line)#exit  
msk-donskaya-vabazlov-gw-1(config)#  
msk-donskaya-vabazlov-gw-1(config)#exit  
msk-donskaya-vabazlov-gw-1#  
%SYS-5-CONFIG_I: Configured from console by console  
  
msk-donskaya-vabazlov-gw-1#wr mem  
Building configuration...  
[OK]  
msk-donskaya-vabazlov-gw-1#
```

Рис. 2.4: Настройка маршрутизатора через CLI

4. Настройка маршрутизатора также проверена с ПК через **Terminal** (консоль-

ный доступ).

В терминале видно выполнение команд включения интерфейса, присвоения IP-адреса, настройки VTY/console, генерации RSA-ключей и сохранения конфигурации.



```
msk-donskaya-vabazlov-gw-1(config-if)#no shut
msk-donskaya-vabazlov-gw-1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
msk-donskaya-vabazlov-gw-1(config-if)#ip addr 192.168.1.254 255.255.255.0
msk-donskaya-vabazlov-gw-1(config-if)#line vty 0 4
msk-donskaya-vabazlov-gw-1(config-line)#pass cisco
msk-donskaya-vabazlov-gw-1(config-line)#login
msk-donskaya-vabazlov-gw-1(config-line)#line console 0
msk-donskaya-vabazlov-gw-1(config-line)#pass cisco
msk-donskaya-vabazlov-gw-1(config-line)#login
msk-donskaya-vabazlov-gw-1(config-line)#enable secret cisco
msk-donskaya-vabazlov-gw-1(config)#serv pass
msk-donskaya-vabazlov-gw-1(config)#user admin priv 1 secret cisco
msk-donskaya-vabazlov-gw-1(config)#tip domain-name donskaya.rudn.edu
msk-donskaya-vabazlov-gw-1(config)#crypto key gen rsa
The name for the keys will be: msk-donskaya-vabazlov-gw-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-vabazlov-gw-1(config)#line vty 0 4
*Mar 1 0:7:51.643: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:7:51.643: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-vabazlov-gw-1(config-line)#tran in ssh
msk-donskaya-vabazlov-gw-1(config-line)#exit
msk-donskaya-vabazlov-gw-1(config)#
msk-donskaya-vabazlov-gw-1(config)#exit
msk-donskaya-vabazlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-vabazlov-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-vabazlov-gw-1#
msk-donskaya-vabazlov-gw-1#
```

Рис. 2.5: Консольный доступ и команды настройки маршрутизатора

## 5. Выполнена настройка коммутатора **msk-donskaya-vabazlov-sw-1**.

Для управления создан виртуальный интерфейс **VLAN2** с IP-адресом **192.168.2.1/24**, интерфейс включён командой **no shutdown**.

Порт **Fa0/1**, к которому подключён ПК, переведён в режим **access** и назначен во **VLAN2**.

Также задан шлюз по умолчанию для удалённого управления:

- ip default-gateway 192.168.2.254

Далее выполнена настройка удалённого администрирования:

- настроены линии VTY (0–4), пароль и вход по логину;
- задан пароль enable (enable secret);
- создан пользователь **admin**;
- задано доменное имя;
- сгенерированы RSA-ключи;
- включён SSH и разрешён только SSH на VTY;
- конфигурация сохранена командой wr mem.

```

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

msk-donskaya-vabazlov-sw-1(config-if)#ip default-gateway 192.168.2.254
msk-donskaya-vabazlov-sw-1(config)#line vty 0 4
msk-donskaya-vabazlov-sw-1(config-line)#pass cisco
msk-donskaya-vabazlov-sw-1(config-line)#login
msk-donskaya-vabazlov-sw-1(config-line)#en secret cisco
* Ambiguous command: "en secret cisco"
msk-donskaya-vabazlov-sw-1(config)#enab secret cisco
msk-donskaya-vabazlov-sw-1(config)#serv pass
msk-donskaya-vabazlov-sw-1(config)#user admin priv 1 secret cisco
msk-donskaya-vabazlov-sw-1(config)#ip domain-name donskaya.rudn.edu
msk-donskaya-vabazlov-sw-1(config)#crypto key gen rsa
The name for the keys will be: msk-donskaya-vabazlov-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-vabazlov-sw-1(config)#line vty 0 4
*Mar 1 0:15:13.469: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:15:13.469: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-donskaya-vabazlov-sw-1(config-line)#tra in ssh
msk-donskaya-vabazlov-sw-1(config-line)#exit
msk-donskaya-vabazlov-sw-1(config)#exit
msk-donskaya-vabazlov-sw-1#
*SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-vabazlov-sw-1#wr mem
Building configuration...
[OK]
msk-donskaya-vabazlov-sw-1#

```

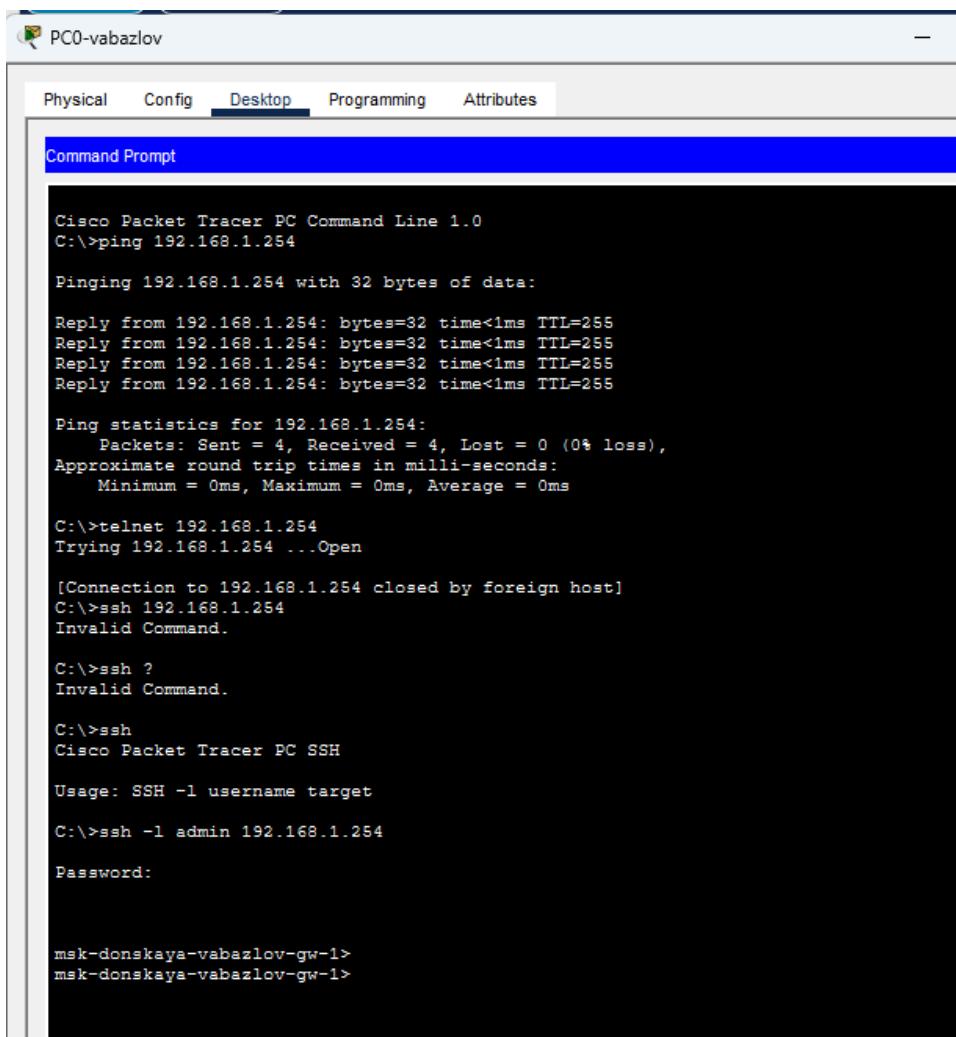
Рис. 2.6: Настройка коммутатора через CLI

6. Проверена доступность маршрутизатора с ПК **PC0-vabazlov** командой **ping** на адрес **192.168.1.254**.

Получены ответы на ICMP-запросы без потерь, что подтверждает корректность IP-настройки и работоспособность канала связи.

Далее выполнена попытка подключения к маршрутизатору разными способами:

- **telnet 192.168.1.254** – соединение устанавливается, но закрывается удалённой стороной (что типично при ограничениях/настройках VTY);
- **ssh -l admin 192.168.1.254** – успешный вход после ввода пароля.



The screenshot shows a Cisco Packet Tracer Command Line interface window titled 'PC0-vabazlov'. The tabs at the top are Physical, Config, Desktop (which is selected), Programming, and Attributes. The command prompt is labeled 'Command Prompt'. The terminal window displays the following 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 192.168.1.254
Invalid Command.

C:\>ssh ?
Invalid Command.

C:\>ssh
Cisco Packet Tracer PC SSH

Usage: SSH -l username target

C:\>ssh -l admin 192.168.1.254

Password:

msk-donskaya-vabazlov-gw-1>
msk-donskaya-vabazlov-gw-1>
```

Рис. 2.7: Ping и удалённый доступ к маршрутизатору (Telnet/SSH)

7. Проверена доступность коммутатора с ПК **PC1-vabazlov** командой **ping** на

адрес **192.168.2.1**.

После получения ответов выполнено подключение к коммутатору:

- **telnet 192.168.2.1** – соединение открывается и затем закрывается удалённой стороной;
- **ssh -l admin 192.168.2.1** – успешное подключение по SSH после ввода пароля, доступ к CLI подтверждён.

```
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-vabazlov-sw-1>exit

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

Рис. 2.8: Ping и удалённый доступ к коммутатору (Telnet/SSH)

## 3 Контрольные вопросы

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

Подключение к сетевому оборудованию может осуществляться нескольки-ми способами:

**Консольное подключение** – выполняется с помощью консольного кабеля напрямую от ПК к устройству (Console port). Используется для первоначальной настройки, когда у устройства ещё нет IP-адреса или удалённый доступ не настроен.

**Подключение по Telnet** – удалённый доступ по сети с использованием IP-адреса устройства. Позволяет управлять оборудованием через командную строку, но передаёт данные, включая пароли, в незашифрованном виде.

**Подключение по SSH** – удалённый доступ по сети с шифрованием. Обеспечивает безопасное управление устройством и защищает передаваемые данные от перехвата.

**Подключение через веб-интерфейс (HTTP/HTTPS)** – используется на устройствах с графическим интерфейсом управления. Позволяет настраивать оборудование через браузер.

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

Для подключения ПК к маршрутизатору обычно используется медный прямой кабель (Copper Straight-Through).

Это связано с тем, что соединяются разные типы устройств: оконечное устройство (ПК) и сетевое устройство (маршрутизатор). У таких устройств различается назначение контактов передачи и приёма, поэтому прямой кабель обеспечивает корректное соединение без перекрёстной коммутации проводов.

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

В данном случае также используется медный прямой кабель (Copper Straight-Through).

ПК и коммутатор относятся к разным типам устройств: один передаёт данные как конечный узел, второй — как сетевое устройство. Прямой кабель позволяет корректно соединить контакты передачи и приёма между ними.

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

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

Это связано с тем, что соединяются однотипные устройства, у которых линии передачи и приёма совпадают по расположению. Перекрёстный кабель меняет местами соответствующие пары проводов, обеспечивая правильную передачу данных.

В современных устройствах часто используется технология Auto-MDIX, которая автоматически определяет тип подключения, поэтому может работать и прямой кабель.

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

Доступ по паролю можно настроить несколькими способами:

**Пароль для консоли (line console 0)** — защищает локальный доступ через консольный кабель.

**Пароль для виртуальных терминалов (line vty 0–4)** — используется при удалённом подключении по Telnet или SSH.

**Enable password / enable secret** — пароль для входа в привилегированный режим. При этом enable secret считается более безопасным, так как хранится в зашифрованном виде.

**Локальные учётные записи (username + password/secret)** — создание пользователей с логином и паролем для авторизации при удалённом доступе.

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

Основные способы удалённого доступа:

**Telnet** — позволяет подключаться к устройству по сети и управлять им через CLI. Прост в настройке, но не обеспечивает защиты данных, так как вся информация передаётся в открытом виде.

**SSH** — обеспечивает удалённый доступ с использованием шифрования. Требует создания пользователя, доменного имени и RSA-ключей, но значительно повышает безопасность.

**Веб-доступ (HTTP/HTTPS)** — применяется для устройств с графическим интерфейсом. HTTPS предпочтительнее, так как использует шифрование.

Наиболее предпочтительным способом является **SSH**, так как он обеспечивает конфиденциальность передаваемых данных, защищает пароли и команды от перехвата и соответствует современным требованиям безопасности.

## 4 Заключение

В ходе работы была выполнена сборка и настройка простой сети в Cisco Packet Tracer с использованием маршрутизатора, коммутатора и двух оконечных устройств. Проведено подключение оборудования в логической рабочей области и выполнена базовая конфигурация сетевых параметров.

На компьютерах заданы статические IP-адреса, маски подсети и шлюзы по умолчанию. На маршрутизаторе настроен сетевой интерфейс с назначением IP-адреса и включением передачи данных. На коммутаторе создан управляющий интерфейс VLAN, назначен IP-адрес и задан шлюз по умолчанию для удалённого управления.

Дополнительно выполнена настройка параметров безопасности: заданы пароли для консольного доступа и виртуальных терминалов, создана локальная учётная запись администратора, настроен привилегированный режим, сгенерированы RSA-ключи и включён доступ по протоколу SSH.

Работоспособность сети проверена с помощью команды ping, что подтвердило корректность выполненных настроек и доступность сетевых устройств. Выполнено подключение к маршрутизатору и коммутатору различными способами: через консоль, а также по протоколам удалённого доступа Telnet и SSH. Успешное подключение по SSH показало корректность настройки безопасного удалённого управления.

В результате работы были получены практические навыки настройки сетевого оборудования, организации базовой адресации, обеспечения удалённого администрирования и проверки сетевой связности. Полученные знания могут

быть использованы при дальнейшем изучении принципов построения и защиты компьютерных сетей.