

# **Лабораторная работа №2**

**Предварительная настройка оборудования Cisco**

Шияпова Дарина Илдаровна

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>7</b>
3.1	Настройка маршрутизатора . . . . .	8
3.2	Настройка коммутатора . . . . .	11
<b>4</b>	<b>Выводы</b>	<b>14</b>
<b>5</b>	<b>Контрольные вопросы</b>	<b>15</b>

## Список иллюстраций

3.1	Схема подключения оборудования для проведения его предвари- тельной настройки . . . . .	7
3.2	Задание статического ip-адреса PC0 . . . . .	8
3.3	Задание имени оборудованию . . . . .	8
3.4	Задание интерфейсу Fast Ethernet с номером 0 ip-адреса . . . . .	9
3.5	Проверка соединения с помощью команды ping . . . . .	9
3.6	Задание паролей . . . . .	9
3.7	Шифрование паролей . . . . .	10
3.8	Задание доступа 1-го уровня по паролю пользователю admin . . .	10
3.9	Настройка доступа через telnet и ssh . . . . .	10
3.10	Проверка работы доступа через telnet и ssh . . . . .	11
3.11	Задание статического ip-адреса PC2 . . . . .	11
3.12	Задание имени оборудованию . . . . .	12
3.13	Привязка интерфейса Fast Ethernet с номером 1 к vlan 2 . . . . .	12
3.14	Задание в качестве адреса шлюза адрес 192.168.2.254 . . . . .	12
3.15	Проверка соединения с помощью команды ping . . . . .	13

# 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»;
- 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.

2. Сделать предварительную настройку коммутатора:

- задать имя в виде «город-территория-учётная\_записьтип\_оборудования-номер»
- 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

В логической рабочей области Packet Tracer разместим коммутатор, маршрутизатор и 2 оконечных устройства типа PC, соединим один PC с маршрутизатором консольным и кроссовым кабелем, другой PC — с коммутатором консольным и прямым кабелем (рис. 3.1).

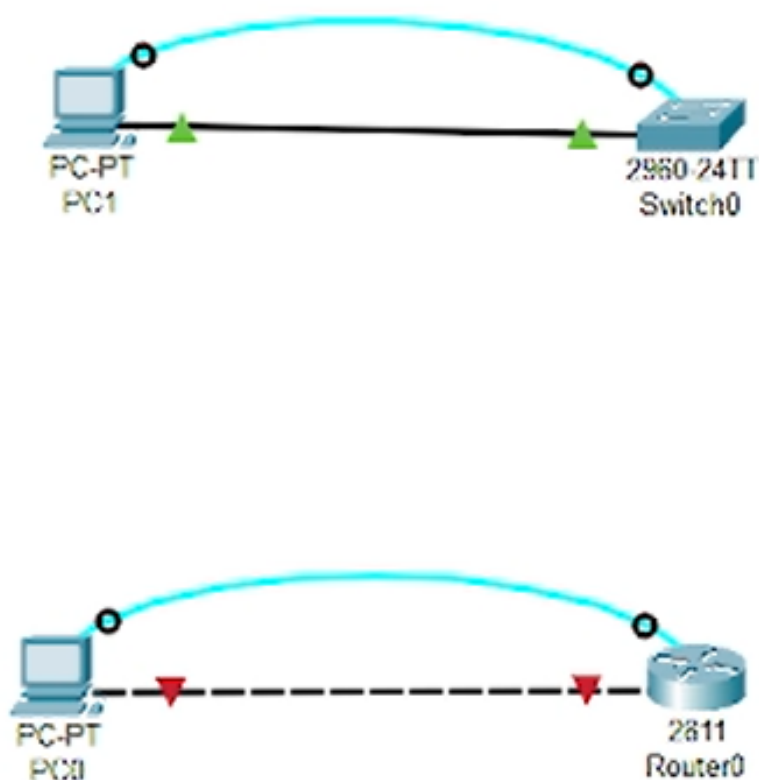


Рис. 3.1: Схема подключения оборудования для проведения его предварительной настройки

Для начала зададим статический ip-адрес PC0 192.168.1.10 с соответствующей маской подсети 255.255.255.0 (рис. 3.2).

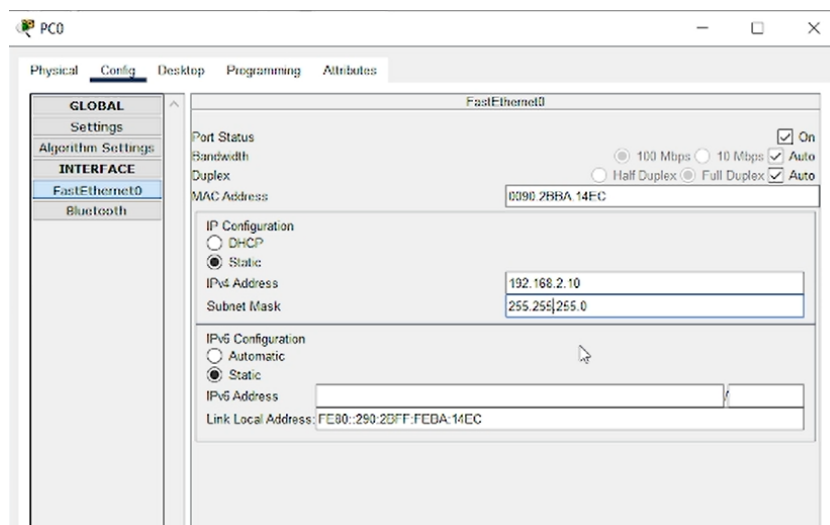


Рис. 3.2: Задание статического ip-адреса PC0

## 3.1 Настройка маршрутизатора

Теперь проведем настройку маршрутизатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Для перехода в привилегированный режим из пользовательского режима воспользуемся командой `enable`. А для перехода в режим глобальной конфигурации из привилегированного режима используем команду `configure terminal` или её сокращённый аналог `conf t`. И в этом режиме зададим имя хоста, введя команду `hostname msk-donskaya-gw-1` (рис. 3.3).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname mas-chertanovo-gw-1
```

Рис. 3.3: Задание имени оборудованию

Зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем интерфейс командой `no shutdown` (рис. 3.4).



```

msk-chertanovo-gw-1(config)#interface f0/0
msk-chertanovo-gw-1(config-if)#no shutdown
msk-chertanovo-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-chertanovo-gw-1(config-if)#line vty 0 4
msk-chertanovo-gw-1(config-line)#password cisco
msk-chertanovo-gw-1(config-line)#login
msk-chertanovo-gw-1(config-line)#line console 0

```

Рис. 3.4: Задание интерфейсу Fast Ethernet с номером 0 ip-адреса

Проверим работоспособность соединения с помощью команды ping. Увидим, что было послано 4 пакета и принято тоже 4, потерь нет. Так что соединение успешно работает (рис. 3.5).

```

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

```

Рис. 3.5: Проверка соединения с помощью команды ping

Зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном). Зададим пароль для доступа к терминалу, к консоли, и поставим пароль на enable (привилегированным режим) (рис. 3.6).

```

msk-chertanovo-gw-1(config-if)#line vty 0 4
msk-chertanovo-gw-1(config-line)#password cisco
msk-chertanovo-gw-1(config-line)#login
msk-chertanovo-gw-1(config-line)#line console 0
msk-chertanovo-gw-1(config-line)#password cisco
msk-chertanovo-gw-1(config-line)#login
msk-chertanovo-gw-1(config-line)#enable secret cisco

```

Рис. 3.6: Задание паролей

Если использовать команду secret, то пароль сразу будет зашифрованным. Но там, где мы использовали команду password пароль не скрыт, и любой может его посмотреть. Чтобы это исправить, надо зашифровать наши пароли с помощью команды service password -encryption (рис. 3.7).

```
msk-chertanovo-gw-1(config-line)#enable secret cisco
msk-chertanovo-gw-1(config)#service password-encryption
msk-chertanovo-gw-1(config)#username admin privilege 1 secret cisco
msk-chertanovo-gw-1(config)#ip domain name donskaya.rudn.edu
msk-chertanovo-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-chertanovo-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.
```

Рис. 3.7: Шифрование паролей

В качестве дополнительного уровня защиты для пользователя admin зададим доступ 1-го уровня по паролю (рис. 3.8).

```
msk-chertanovo-gw-1(config)#username admin privilege 1 secret cisco
```

Рис. 3.8: Задание доступа 1-го уровня по паролю пользователю admin

Теперь настроим доступ к оборудованию сначала через telnet, затем — через ssh (используя в качестве имени домена donskaya.rudn.edu) (рис. 3.9).

```
The name for the keys will be: msk-chertanovo-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]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

msk-chertanovo-gw-1(config)#line vty 0 4
*Mar 1 0:22:15.89: RSA key size needs to be at least 768 bits for ssh version 2
*Mar 1 0:22:15.90: %SSH-5-ENABLED: SSH 1.5 has been enabled
msk-chertanovo-gw-1(config-line)#transport input ssh

% Invalid input detected at '^' marker.

msk-chertanovo-gw-1(config-line)#transport input ssh
```

Рис. 3.9: Настройка доступа через telnet и ssh

Так как мы оставили возможным доступ только через ssh, то при попытке доступа через telnet нам будет отказано. А при доступе через ssh запрашивается пароль, как и должен, и доступ успешно предоставляется (рис. 3.10).

```
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
Invalid Command.

C:\>ssh -l admin 192.168.1.251

* Connection timed out; remote host not responding
C:\>ssh -l admin 192.168.1.254

Password:

msk-chertanovo-gw-1>exit

[Connection to 192.168.1.254 closed by foreign host]
```

Рис. 3.10: Проверка работы доступа через telnet и ssh

Наконец сохраним нашу конфигурацию маршрутизатора.

## 3.2 Настройка коммутатора

Для начала зададим статический ip-адрес PC0 192.168.2.10 с соответствующей маской подсети 255.255.255.0 (рис. 3.11).

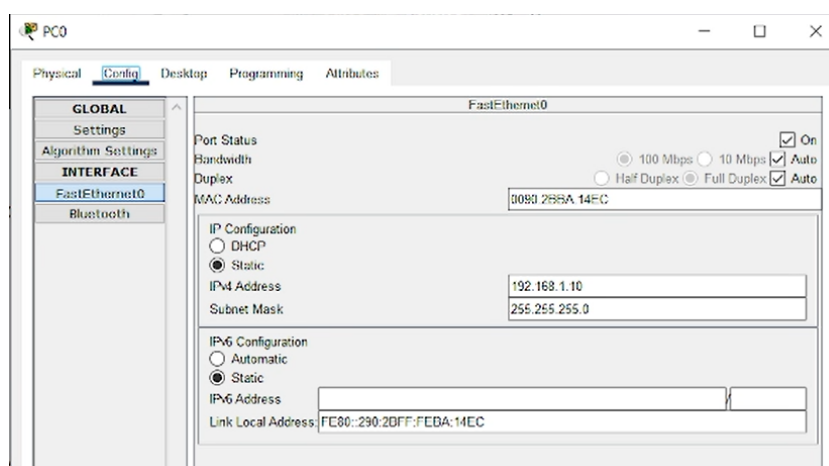


Рис. 3.11: Задание статического ip-адреса PC2

Теперь проведем настройку коммутатора в соответствии с заданием. Откроем Command Line Interface (CLI) у маршрутизатора, который идентичен терминалу ПК. Для перехода в привилегированный режим из пользовательского режима воспользуемся командой `enable`. А для перехода в режим глобальной конфигурации из привилегированного режима используем команду `configure terminal` или её сокращённый аналог `conf t`. И в этом режиме зададим имя хоста, введя команду `hostname msk-donskaya-gw-1`. Также зададим интерфейсу Fast Ethernet с номером 0 ip-адрес 192.168.1.254 и маску 255.255.255.0, затем поднимем интерфейс командой `no shutdown` (рис. 3.12).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-chertanovo-sw-1
msk-chertanovo-sw-1(config)#interface vlan2
^
% Invalid input detected at '^' marker.

msk-chertanovo-sw-1(config)#interface vlan2
msk-chertanovo-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-chertanovo-sw-1(config-if)#interface f0/1
```

Рис. 3.12: Задание имени оборудованию

Привяжем интерфейс Fast Ethernet с номером 1 к vlan 2 (рис. 3.13).

```
msk-chertanovo-sw-1(config)#interface vlan2
msk-chertanovo-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-chertanovo-sw-1(config-if)#interface f0/1
msk-chertanovo-sw-1(config-if)#switchport mode access
msk-chertanovo-sw-1(config-if)#switchport mode vlan 2
^
% Invalid input detected at '^' marker.

msk-chertanovo-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-chertanovo-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up
```

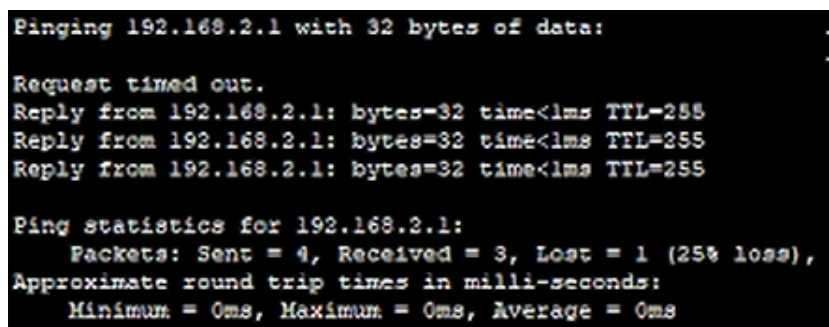
Рис. 3.13: Привязка интерфейса Fast Ethernet с номером 1 к vlan 2

И зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. 3.14).

```
msk-chertanovo-sw-1(config)#ip default-gateway 192.168.2.254
msk-chertanovo-sw-1(config)#exit
```

Рис. 3.14: Задание в качестве адреса шлюза адрес 192.168.2.254

Проверим работоспособность соединения с помощью команды `ping`. Увидим, что было послано 4 пакета и принято тоже 4, потерь нет. Так что соединение успешно работает (рис. 3.15).



```
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
```

Рис. 3.15: Проверка соединения с помощью команды `ping`

Зададим пароль для доступа к привилегированному режиму (сначала в открытом виде, затем — в зашифрованном). Зададим пароль для доступа к терминалу, к консоли, и поставим пароль на `enable` (привилегированным режим). Зашифруем наши пароли с помощью команды `service password -encryption`.

В качестве дополнительного уровня защиты для пользователя `admin` зададим доступ 1-го уровня по паролю.

Теперь настроим доступ к оборудованию сначала через `telnet`, затем — через `ssh` (используя в качестве имени домена `donskaya.rudn.edu`).

Так как мы оставили возможным доступ только через `ssh`, то при попытке доступа через `telnet` нам будет отказано. А при доступе через `ssh` запрашивается пароль, как и должен, и доступ успешно предоставляется.

Сохраним нашу конфигурацию маршрутизатора.

## **4 Выводы**

В процессе выполнения данной лабораторной работы я получила основные навыки по начальному конфигурированию оборудования Cisco.

## 5 Контрольные вопросы

1. Укажите возможные способы подключения к сетевому оборудованию.

Можно подключиться с помощью консольного кабеля или удаленно по ssh или telnet.

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

Кроссовым кабелем

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

Прямым кабелем (витой парой).

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

Кроссовым кабелем (для соединения одиночного оборудования используют кроссовый кабель)

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

С помощью команды password или с помощью команды secret

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

Через telnet или ssh. SSH обеспечивает шифрование и аутентификацию по умолчанию, в отличие от Telnet, который не предоставляет эти функции, поэтому он лучше.