

# **Лабораторная работа 2**

**Предварительная настройка оборудования Cisco**

Ланцова Яна Игоревна

# Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	7
4	Выводы	15
5	Контрольные вопросы	16

## Список иллюстраций

3.1	Схема подключения оборудования . . . . .	7
3.2	Задание статического ip-адреса PC0 . . . . .	8
3.3	Задание статического ip-адреса PC1 . . . . .	8
3.4	Задание имени оборудованию . . . . .	9
3.5	Задание интерфейсу Fast Ethernet с номером 0 ip-адреса . . . . .	9
3.6	Задание паролей и их шифрование . . . . .	10
3.7	Настройка доступа через telnet и ssh . . . . .	10
3.8	Потеря нет, соединение успешно работает . . . . .	11
3.9	Проверка работы доступа через telnet и ssh . . . . .	11
3.10	Задание имени оборудованию и задание интерфейсу Fast Ethernet с номером 0 ip-адреса . . . . .	12
3.11	Привязка интерфейса и задание шлюза . . . . .	12
3.12	Задание и шифрование паролей . . . . .	13
3.13	Настройка доступа через telnet и ssh . . . . .	13
3.14	Потеря нет, соединение успешно работает . . . . .	13
3.15	Проверка работы доступа через telnet и ssh . . . . .	14

# 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. [fig:001?]).

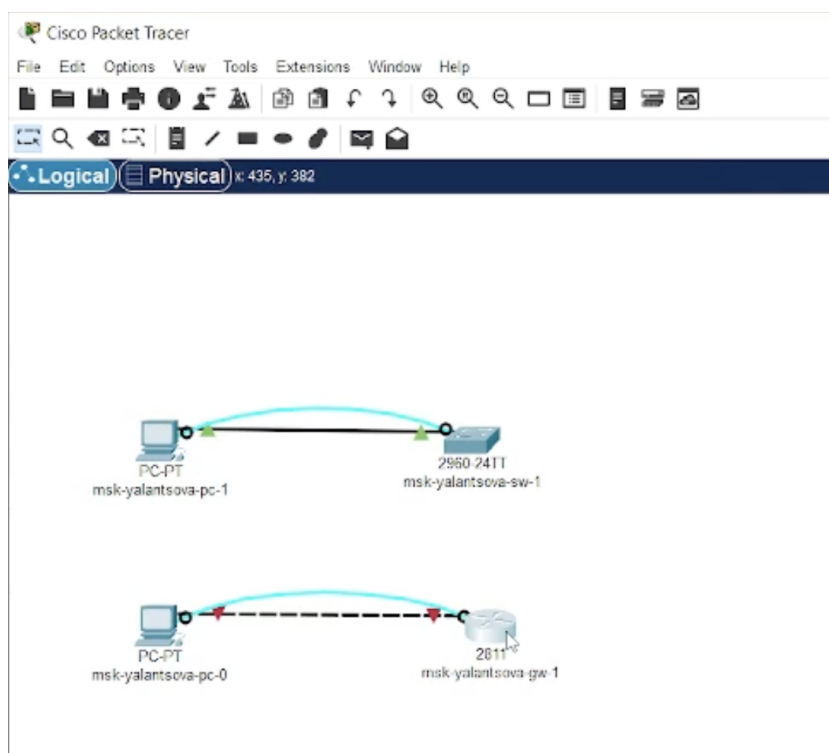


Рис. 3.1: Схема подключения оборудования

Для начала зададим статический ip-адрес PC0 192.168.1.10 с соответствующей маской подсети 255.255.255.0(рис. [fig:002?]).

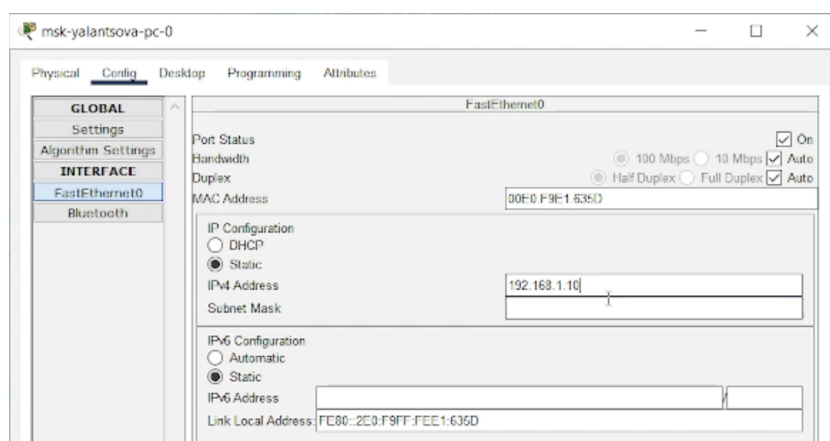


Рис. 3.2: Задание статического ip-адреса PC0

Также зададим статический ip-адрес PC1 192.168.2.10 с соответствующей маской подсети 255.255.255.0 (рис. [fig:003?]):

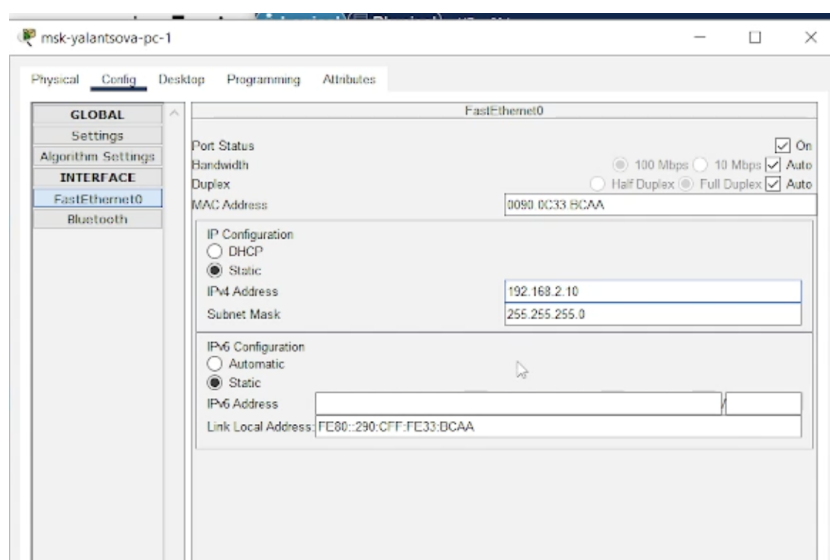


Рис. 3.3: Задание статического ip-адреса PC1

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-valantsova-gw-1` (рис. [fig:004?]).

```
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#
Router(config-if)#hostname msk-valantsova-gw-1
```

Рис. 3.4: 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. [fig:005?]).

```
msk-valantsova-gw-1(config)#interface f0/0
msk-valantsova-gw-1(config-if)#no shutdown

msk-valantsova-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

msk-valantsova-gw-1(config-if)#ip address 192.168.1.254 255.255.255.0
msk-valantsova-gw-1(config-if)#
```

Рис. 3.5: Задание интерфейсу Fast Ethernet с номером 0 ip-адреса

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). Необходимо зашифровать наши пароли с помощью команды `service password -encryption` (рис. [fig:006?]).

```

msk-yalantseva-gw-1(config)#line vty 0 4
msk-yalantseva-gw-1(config-line)#password cisco
msk-yalantseva-gw-1(config-line)#login
msk-yalantseva-gw-1(config-line)#console 0
^
% Invalid input detected at '^' marker.

msk-yalantseva-gw-1(config-line)#line console 0
msk-yalantseva-gw-1(config-line)#password cisco
msk-yalantseva-gw-1(config-line)#login
msk-yalantseva-gw-1(config-line)#enable secret cisco
msk-yalantseva-gw-1(config)#service password encryption
^
% Invalid input detected at '^' marker.

msk-yalantseva-gw-1(config)#service password-encryption
msk-yalantseva-gw-1(config)#

```

Рис. 3.6: Задание паролей и их шифрование

В качестве дополнительного уровня защиты для пользователя `admin` зададим доступ 1-го уровня по паролю. Также настроим доступ к оборудованию сначала через `telnet`, затем — через `ssh` (используя в качестве имени домена `donskaya.rudn.edu`) (рис. [fig:007?]).

```

msk-yalantseva-gw-1(config)#
msk-yalantseva-gw-1(config)#username admin privilege 1 secret cisco
msk-yalantseva-gw-1(config)#ip domain name donskaya.rudn.edu
msk-yalantseva-gw-1(config)#crypto key generate rsa
The name for the keys will be: msk-yalantseva-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]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

msk-yalantseva-gw-1(config)#line vty 0 4
*Mar 1 0:29:54.490: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-yalantseva-gw-1(config-line)#transport input ssh
msk-yalantseva-gw-1(config-line)#

```

Рис. 3.7: Настройка доступа через `telnet` и `ssh`

Проверим соединение с помощью команды `ping` (рис. [fig:008?]).

```
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. 3.8: Потеря нет, соединение успешно работает

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. [fig:009?]).

```
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 -l admin 192.168.1.254

Password:

msk-yalantsova-gw-1>
```

Рис. 3.9: Проверка работы доступа через telnet и ssh

Сохраним конфигурацию маршрутизатора

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-yalantsova-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. [fig:010?]).

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname msk-yalantsova-sw-1
msk-yalantsova-sw-1(config)#interface vlan2
msk-yalantsova-sw-1(config-if)#no shutdown
msk-yalantsova-sw-1(config-if)#ip address 192.168.2.1 255.255.255.0
msk-yalantsova-sw-1(config-if)#
```

Рис. 3.10: Задание имени оборудованию и задание интерфейсу Fast Ethernet с номером 0 ip-адреса

Привяжем интерфейс Fast Ethernet с номером 1 к vlan 2. И зададим в качестве адреса шлюза по умолчанию адрес 192.168.2.254 (рис. [fig:011?]).

```
msk-yalantsova-sw-1(config-if)#interface f0/1
msk-yalantsova-sw-1(config-if)#switchport mode access
msk-yalantsova-sw-1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
msk-yalantsova-sw-1(config-if)#
%LINK-3-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state to up

msk-yalantsova-sw-1(config-if)#ip default gateway 192.168.2.254
^
% Invalid input detected at '^' marker.

msk-yalantsova-sw-1(config-if)#exit
msk-yalantsova-sw-1(config)#ip default gateway 192.168.2.254
^
% Invalid input detected at '^' marker.

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

Рис. 3.11: Привязка интерфейса и задание шлюза

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` (рис. [fig:012?]).

```

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

```

Рис. 3.12: Задание и шифрование паролей

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) (рис. [fig:013?]).

```

msk-yalantsova-sw-1(config)#username admin privilege 1 secret cisco
msk-yalantsova-sw-1(config)#ip domain name donskaya.rudn.edu
msk-yalantsova-sw-1(config)#crypto key generate rsa
The name for the keys will be: msk-yalantsova-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]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

msk-yalantsova-sw-1(config)#line vty 0 4
*Mar 1 0:37:14.585: %SSH-5-ENABLED: SSH 1.99 has been enabled
msk-yalantsova-sw-1(config-line)#transport input ssh
msk-yalantsova-sw-1(config-line)#

```

Рис. 3.13: Настройка доступа через telnet и ssh

Проверим соединение с помощью команды ping (рис. [fig:014?]).

```

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

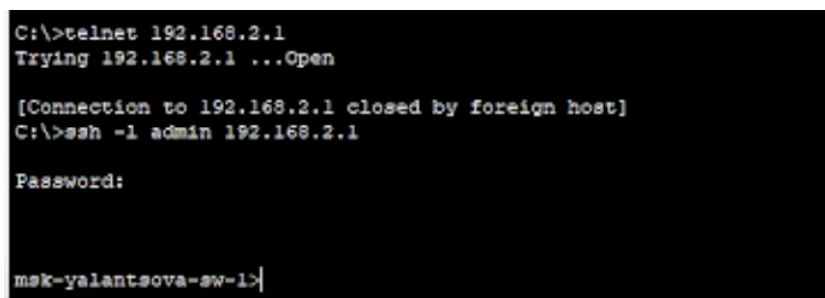
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255

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

```

Рис. 3.14: Потерь нет, соединение успешно работает

Поскольку 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. [fig:015?]).

A screenshot of a Windows command prompt window with a black background and white text. The text shows a sequence of commands and their outputs: first, 'C:\>telnet 192.168.2.1' followed by 'Trying 192.168.2.1 ...Open' and then '[Connection to 192.168.2.1 closed by foreign host]'. Next, the command 'C:\>ssh -l admin 192.168.2.1' is entered, followed by the prompt 'Password:'. Finally, the prompt 'msk-yalantsova-sw-1>' is shown, indicating a successful SSH connection.

```
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-yalantsova-sw-1>
```

Рис. 3.15: Проверка работы доступа через telnet и ssh

Наконец 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), потому что витая пара с разъемами является стандартом для локальных сетей (LAN) Ethernet. Большинство устройств и маршрутизаторов имеют соответствующие порты, что обеспечивает простое и надежное подключение. Витая пара относительно недорогая, что делает её экономически выгодным решением для построения локальных сетей.

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.